SIXTH EDITION

ETHICS IN INFORMATION TECHNOLOGY

GEORGE W. REYNOLDS

ETHICS IN INFORMATION TECHNOLOGY

Sixth Edition

ETHICS IN INFORMATION TECHNOLOGY

Sixth Edition

George W. Reynolds

CENGAGE

Australia • Brazil • Mexico • Singapore • United Kingdom • United States

CENGAGE

Ethics in Information Technology,
Sixth Edition
George W. Reynolds

SVP, GM Science, Technology & Math: Balraj S. Kalsi

Senior Product Director: Kathleen McMahon

Product Team Manager: Kristin McNary

Associate Product Manager: Kate Mason

Senior Director, Development: Julia Caballero

Senior Content Development Manager: Leigh Hefferon

Associate Content Developer: Maria Garguilo

Product Assistant: Jake Toth

VP, Marketing for Science, Technology, & Math: Jason Sakos

Marketing Director: Michele McTighe

Marketing Manager: Stephanie Albracht

Production Director: Patty Stephan

Content Project Manager: Michele Stulga

Art Director: Diana Graham

Cover Designer: Roycroft Design (roycroftdesign.com)

Cover Image: iStock.com/sumkinn

Library of Congress Control Number: 2017950121

ISBN: 978-1-337-40587-4

Cengage
20 Channel Street
Boston, MA 02210
USA

Notice to the Reader

Publisher does not warrant or guarantee any of the products described herein or perform any independent analysis in connection with any of the product information contained herein. Publisher does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. The publisher makes no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and the publisher takes no responsibility with respect to such material. The publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or part, from the readers' use of, or reliance upon, this material.

Printed in the United States of America
Print Number: 01   Print Year: 2017

BRIEF CONTENTS

TABLE OF CONTENTS

PREFACE

We are excited to publish the sixth edition of *Ethics in Information Technology*. This new edition builds on the success of the previous editions and meets the need for a resource that helps readers understand many of the legal, ethical, and societal issues associated with information technology. We have responded to the feedback from our previous edition adopters, students, and other reviewers to create an improved text. We think you will be pleased with the results.

Ethics in Information Technology, Sixth Edition, fills a void of practical business information for business managers and IT professionals. The typical introductory information systems book devotes one chapter to ethics and IT, which cannot possibly cover the full scope of ethical issues related to IT. Such limited coverage does not meet the needs of business managers and IT professionals—the people primarily responsible for addressing ethical issues in the workplace. What is missing is an examination of the different ethical situations that arise in IT as well as practical advice for addressing these issues.

Ethics in Information Technology, Sixth Edition, has enough substance for an instructor to use it in a full-semester course in computer ethics. Instructors can also use the book as a reading supplement for such courses as Introduction to Management Information Systems, Principles of Information Technology, Managerial Perspective of Information Technology, Computer Security, E-Commerce, and so on.

WHAT'S NEW

Ethics in Information Technology, Sixth Edition, has been updated and revised to incorporate the many new developments and ethical issues that are affecting IT professionals and influencing professional ethics, such as state licensing of IT professionals; cyberterrorism and hacktivism; the erosion of privacy due to electronic surveillance; the positive and negative impacts of social networking; the design and implementation of safety-critical systems; and the impact of IT on the standard of living, worker productivity, and health care.

Each chapter opens with a new "Organizations Behaving Badly" real-world scenario that highlights key issues from the chapter and raises thought-provoking questions. Critical thinking exercises, also a new feature, are strategically placed at the end of each major chapter section to encourage the reader to pause, consider, and apply what they've just read. Each chapter ends with a list of key terms and a set of self-assessment questions that students can use to check their grasp of key points from the chapter. New—and more varied—end-of-chapter exercises have been added to encourage critical application of chapter concepts. Students can practice principles they've learned with revised Discussion Questions, and What Would You Do? exercises, as well as all new Cases. Instructors of online courses can use this wealth of material as the basis for discussion forums that allow their online students to share a variety of perspectives and experiences and to create a learning community. Such discussions provide students the opportunity to more deeply understand the material while challenging their critical thinking skills. We think you will like these changes and additions.

ORGANIZATION

Each of the 10 chapters in this book addresses a different aspect of ethics in information technology:

- Chapter 1, "An Overview of Ethics," introduces ethics, ethics in business, and the importance of ethics in IT. The distinction between morals, ethics, and laws is defined. The trends that have increased the likelihood of unethical behavior are identified. The concept of corporate social responsibility is defined and discussed. The chapter presents reasons why practicing good business ethics is important in business. A model for improving corporate ethics is provided. The most commonly observed types of misconduct in the workplace are identified. The need for an organizational code of ethics is discussed. Key steps in establishing a sound ethics program are outlined. The role of the chief ethics officer and board of directors in establishing a strong organizational ethics program is examined. A useful model for ethical decision making is provided. The chapter ends with a discussion of the role of ethics in IT.
- Chapter 2, "Ethics for IT Workers and IT Users," explains the importance of ethics in the business relationships of IT professionals, including those between IT workers and employers, clients, suppliers, other professionals, IT users, and society. The chapter provides suggestions for what can be done to encourage the professionalism of IT workers by emphasizing the significance of IT professional organizations and their codes of ethics as well as certification and licensing. Some ethical issues faced by IT users are discussed, including software piracy, inappropriate use of computing resources, and inappropriate sharing of information. Actions that can be taken to encourage the ethical use of IT resources by end-users are outlined. The chapter introduces the topic of internal control and compliance and the role the audit committee and members of the internal audit team have in ensuring that both the IT organization and IT users follow organizational guidelines and policies, as well as various legal and regulatory practices.
- Chapter 3, "Cyberattacks and Cybersecurity," describes the types of ethical decisions that IT professionals must make, as well as the business needs they must balance when dealing with security issues. The chapter identifies the most common computer-related security incidents and provides numerous reasons why such incidents are increasing. This chapter includes information on the use of cloud computing, virtualization software, and bring your own device corporate business policies. It describes some of the more common hacker attacks, including ransomware, viruses, worms, Trojan horses, blended threats, distributed denial-of-service, rootkits, advanced persistent

threats, spam, phishing, spear-phishing, smishing, and vishing. Cyberespionage and cyberterrorism are also covered including the roles of the United States Computer Emergency Readiness Team (US-CERT) and the Department of Homeland Security in defending against cyberterrorism. In addition to providing a useful classification of computer crimes and their perpetrators, the chapter summarizes the major federal laws that address computer crime. The chapter introduces the concept of the CIA triad (confidentiality, integrity, and availability) and outlines steps to implement this concept throughout the organization at all levels. The chapter discusses the need for a corporate security policy and offers both a process for establishing a security policy and several security-related policy templates that can help an organization to quickly develop effective security policies. A process for performing an assessment of an organization's IT resources from both internal and external threats is presented. Useful guidelines are provided on how to respond to specific security incidents to quickly resolve problems and improve ongoing security measures.

- Chapter 4, "Privacy," explains how the use of IT affects privacy rights and discusses several key pieces of legislation that have addressed privacy rights over the years. The Fourth Amendment is explained, and laws designed to protect personal financial and health data—as well as the privacy of children—are discussed. Electronic surveillance is covered, along with many laws associated with this activity, including Executive Order 12333, the Foreign Intelligence Surveillance Act, and the USA PATRIOT Act including its various amendments and extensions. Various regulations affecting the export of personal data from one country to another are covered. The chapter explains how the personal information businesses gather using IT can be used to obtain or keep customers (or to monitor employees). It also discusses the concerns of privacy advocates regarding how much information can be gathered, with whom it can be shared, how the information is gathered in the first place, and how it is used. These concerns also extend to the information-gathering practices of law enforcement and government. Identity theft and data breaches are covered along with various tactics used by identity thieves; the chapter also presents some safeguards that can thwart identity theft. Guidelines and principles for treating consumer data responsibly are offered. The pros and cons of consumer profiling as well as various tactics for profiling are discussed. The expanding use of electronic discovery, workplace monitoring, camera surveillance, vehicle data recorders, and stalking apps is discussed.
- Chapter 5, "Freedom of Expression," addresses issues raised by the growing use of the Internet as a means for freedom of expression, while also examining the types of speech protected by the First Amendment of the U.S. Constitution. The chapter covers the ways in which the ease and anonymity with which Internet users can communicate may pose problems for people who might be adversely affected by such communications. It describes attempts at using legislation (such as the Communications Decency Act, the Children Online Protection Act, and the Children's Internet Protection Act) and

technology, such as Internet filtering, to control access to Internet content that is unsuitable for children or unnecessary in a business environment. The use of strategic lawsuits against public participation (SLAPP) lawsuits is covered. The use of John Doe lawsuits to reveal the identities of anonymous posters is discussed. Internet censorship, doxing, sexting, fake news, defamation, hate speech, pornography on the Internet, and spam are also covered.

- Chapter 6, “Intellectual Property,” defines intellectual property and explains the varying degrees of ownership protection offered by copyright, patent, and trade secret laws. Copyright, patent, and trademark infringement are examined, using many examples. Key U.S. and international rules aimed at protecting intellectual property are discussed, including the Prioritizing Resources and Organization for Intellectual Property Act, the General Agreement on Tariffs and Trade, the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights, the World Intellectual Property Organization Copyright Treaty, and the Digital Millennium Copyright Act. The chapter explains software patents and software licensing as well as the use of cross-licensing agreements. It also addresses key intellectual property issues such as plagiarism, reverse engineering, open source code, competitive intelligence, trademark infringement, and cybersquatting. The use of nondisclosure agreements and noncompete clauses in work contracts is also discussed. Finally, the chapter addresses several key issues relevant to ethics in IT, including plagiarism, reverse engineering of software, open source code, competitive intelligence gathering, and cybersquatting.
- Chapter 7, “Ethical Decisions in Software Development,” provides a thorough discussion of the software development process and the importance of software quality. It covers the ethical and economic issues that software manufacturers must consider when deciding “how good is good enough?” with regard to their software products—particularly when the software is safety-critical and its failure can cause loss of human life. Topics include software product liability, risk management, quality management, and quality assurance. An overview of and the pros and cons of the waterfall and agile software development approaches are presented. The chapter also examines the Capability Maturity Model Integration (CMMI), the ISO 9000 family of standards, and the Failure mode and effects analysis (FMEA) technique as strategies for improving software quality.
- Chapter 8, “The Impact of Information Technology on Society,” examines the effect that IT investment has had on the standard of living and worker productivity. Also covered are how advances in artificial intelligence, machine learning, robotics, and natural language processing are fundamentally changing the way work gets done and have the potential to affect the tasks, roles, and responsibilities of most workers. The chapter looks at the impact of IT on the delivery of health care and healthcare costs. Electronic medical records, electronic health records, and health information exchanges are explained. The issues with implementing a successful electronic health records system

are discussed. Telehealth and telemedicine are defined and how they help deliver of health care are discussed.

- Chapter 9, "Social Media," discusses how people use social media, identifies common business uses of social media, and examines many of the ethical issues associated with the use of social media. The most popular social networking platforms are identified. The business applications of social media are covered, including the use of social networks to communicate and promote the benefits of products and services, the use of social media in the hiring process, improving customer service, and the creation of social shopping platforms. Common ethical issues that arise for members of social networking platforms including online abuse, harassment, stalking, cyberbullying, encounters with sexual predators, the uploading of inappropriate material, and the inappropriate participation of employees in social networking are discussed. Other social networking issues covered include the increased risk of accidents associated with social media interaction while driving, the tendency of many social media users to become narcissist in their postings, and the ability to perform self-image manipulation.
- Chapter 10, "Ethics of IT Organizations," covers a range of ethical issues facing IT organizations, including those associated with the use of nontraditional workers, such as temporary workers, contractors, consulting firms, H-1B workers, and the use of outsourcing and offshore outsourcing. Also raised is the issue of discriminatory hiring practices at many large IT firms and the special issues of independent contractors working in the gig economy. Factors that are considered in classifying a worker as either an employee or an independent contractor are provided. The chapter also discusses the risks, protections, and ethical decisions related to whistle-blowing, and it presents a process for safely and effectively handling a whistle-blowing situation. In addition to introducing the concept of green computing, the chapter discusses the ethical issues that both IT manufacturers and IT users face when a company is considering how to transition to green computing—and at what cost. It discusses the use of the Electronic Product Environment Assessment Tool to evaluate, compare, and select electronic products based on a set of 51 environmental criteria.
- Appendix A provides an in-depth discussion of how ethics and moral codes developed over time.

PEDAGOGY

Ethics in Information Technology, Sixth Edition, employs a variety of pedagogical features to enrich the learning experience and provide interest for the instructor and student:

- **Opening Quotation.** Each chapter begins with a quotation to stimulate interest in the chapter material.
- **Organizations Behaving Badly.** At the beginning of each chapter, a brief real-world scenario illustrates the issues to be discussed, and carefully crafted focus questions pique the reader's interest.

- **Learning Objectives.** Learning Objectives appear at the start of each chapter. They are presented in the form of questions for students to consider while reading the chapter.
- **Critical Thinking Exercises**. New, thought-provoking critical thinking exercises are strategically placed at the end of each major chapter section to encourage the reader to pause, consider, and apply what they've just read.
- **Key Terms.** Key terms appear in bold in the text and are listed at the end of the chapter. They are also defined in the glossary at the end of the book.
- **Manager's Checklist.** Chapters include a checklist that provides a practical and useful list of questions to consider when making a business decision involving the topics just covered.

End-of-Chapter Material

To help students retain key concepts and expand their understanding of important IT concepts and relationships, the following features are included at the end of every chapter:

- **Summary.** Each chapter includes a summary of the key issues raised that correlate to the Learning Objectives for each chapter.
- **Self-Assessment Questions.** These questions help students review and test their understanding of key chapter concepts. The answers to the Self-Assessment Questions are provided at the end of each chapter.
- **Discussion Questions.** These open-ended questions help instructors generate class discussion to move students deeper into the concepts and help them explore the numerous aspects of ethics in IT.
- **What Would You Do?** These exercises present realistic dilemmas that encourage students to think critically about the ethical principles presented in the text.
- **Cases.** In each chapter, two new real-world cases reinforce important ethical principles and IT concepts, and show how real companies have addressed ethical issues associated with IT. Questions after each case focus students on its key issues and ask them to apply the concepts presented in the chapter.

ABOUT THE AUTHOR

George W. Reynolds brings a wealth of computer and industrial experience to this project, with more than 30 years of experience in government, institutional, and commercial IT organizations with NASA, the Jet Propulsion Laboratory, University of Cincinnati, Procter & Gamble, and Atos. He has authored over two dozen texts and has taught at the University of Cincinnati, Xavier University (Ohio), Miami University (Ohio), the College of Mount St. Joseph, and Strayer University.

Teaching Tools

The following supplemental materials are available when this book is used in a classroom setting. All Instructor Resources can be accessed online at www.cengage.com/login.

- **Instructor's Manual.** Includes additional instructional material to assist in class preparation, including suggestions for lecture topics. It also includes solutions to all end-of-chapter exercises.
- **Test Banks.** Cengage Learning Testing powered by Cognero is a flexible, online system that allows instructors to author, edit, and manage test bank content from multiple Cengage Learning solutions and to create multiple versions. It works on any operating system or browser with no special installs or downloads needed, so tests can be created from anywhere with Internet access.
- **PowerPoint Presentations.** Lecture slides for each chapter can be included as a teaching aid for classroom presentation, made available to students on the network for chapter review, or printed for classroom distribution. The slides are fully customizable. Instructors can either add their own slides for additional topics they introduce to the class or delete slides they won't be covering.
- **Additional Cases.** Find over 40 additional real-world cases to choose from to reinforce important ethical principles and IT concepts, and show how real companies have addressed ethical issues associated with IT. Questions after each case focus students on its key issues and ask them to apply the concepts presented in the chapter.

ACKNOWLEDGMENTS

I wish to express my appreciation to a number of people who helped greatly in the creation of this text: Kristin McNary, Product Team Manager, for her belief in and encouragement of this project; Michele Stulga, Content Project Manager, for guiding the book through the production process; Kate Mason, Associate Product Manager, for overseeing and directing this effort; Maria Garguilo, Associate Content Developer for her outstanding support in all the many activities associated with a project of this scope; Mary Pat Shaffer, Development Editor, for her tremendous support, many useful suggestions, and helpful edits; and the many students and instructors who provided excellent ideas and constructive feedback on the text. I also wish to thank Clancy Martin for writing Appendix A.

Last of all, thanks to my family for all their support, and for giving me the time to write this text.

—George W. Reynolds

CHAPTER 1

AN OVERVIEW OF ETHICS

QUOTE

This above all: to thine own self be true, and it must follow, as the night the day, thou canst not then be false to any man.

—Polonius, a character in *Hamlet*, discussing the importance of integrity with his son, Laertes

Jacek Dudzinski/Shutterstock.com

ORGANIZATIONS BEHAVING BADLY

Ever get upset trying to make sense of all the miscellaneous charges that appear each month on your cell phone bill? Well, it turns out you—and millions of other consumers—may have cause for concern.

In October 2014, the Federal Communications Commission (FCC) announced a $105 million settlement with AT&T Mobility in a case related to the practice of “cramming,” in which unauthorized, recurring third-party charges are added to consumers’ cell phone bills for “premium” subscriptions such as ring tones, wallpaper, and horoscope text messaging services. Often, consumers were duped into signing up for these services without understanding that they would result in ongoing charges, up to $9.99 per month. In addition to allowing third-party companies to place charges on its customers’ accounts without their knowledge, AT&T Mobility lumped together several miscellaneous charges on its bills, making it difficult for customers to detect the unauthorized charges. When customers complained, AT&T Mobility would typically only refund a portion of the cramming charges.[1]

A year later, the FCC fined AT&T Mobility $100 million for misleading customers about its “unlimited” mobile data plans. The FCC alleged that the carrier slowed down the data speeds for customers with such plans after they had used a certain amount of data, a practice called throttling, meaning that these customers were being billed for services they were not receiving in full.[2]

AT&T Mobility is not the only mobile carrier to be fined by the FCC for issues related to their billing practices. In late 2014, T-Mobile USA was fined $90 million for cramming customer phone bills with unauthorized charges for years and then ignoring complaints and requests for refunds.[3] The FCC also fined Verizon $90 million and Sprint $68 million in 2015 for billing customers for third-party texting services without their consent.[4]

The people who developed, implemented, and supported the practice of cramming customer phone bills were once new hires—likely full of ambition and a desire to do well in their jobs. What might cause employees to support and implement a practice, such as cramming, that appears unethical and possibly illegal? What happened to their desire to do well that they did not object to and stop this unfair billing practice? Do you feel pressured to commit such practices in your current place of employment?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What is ethics?
2. What trends have increased the likelihood of an unethical behavior?
3. What is corporate social responsibility, and why is fostering good business ethics important?
4. What measures can organizations take to improve their business ethics?
5. How can you include ethical considerations in your decision making?
6. What trends have increased the risk that information technology will be used in an unethical manner?

WHAT IS ETHICS?

Ethics is a code of behavior that is defined by the group to which an individual belongs. Ethical behavior conforms to generally accepted norms, which may change over time to meet the evolving needs of the society or a group of people who share similar laws, traditions, and values that provide structure to enable them to live in an organized manner. Ethics help members of a group understand their roles and responsibilities so they can work together to achieve mutual benefits such as security, access to resources, and the pursuit of life goals.

Morals are the personal principles upon which an individual bases his or her decisions about what is right and what is wrong. They are core beliefs formed and adhered to by an individual. For example, many of us have a core belief that all people should be treated with respect and this belief governs our actions toward others. Your moral principles are statements of what you believe to be rules of right conduct. As a child, you may have been taught not to lie, cheat, or steal. As an adult facing more complex decisions, you often reflect on your moral principles when you consider what to do in different situations: Is it okay to lie to protect someone's feelings? Should you intervene with a coworker who seems to have a chemical dependency problem? Is it acceptable to exaggerate your work experience on a résumé? Can you cut corners on a project to meet a tight deadline?

As children grow, they learn complicated tasks—such as walking, talking, swimming, riding a bike, and writing the alphabet—that they perform out of habit for the rest of their lives. People also develop habits that make it easier for them to choose between good and bad. A **virtue** is a habit that inclines people to do what is acceptable, and a **vice** is a habit of unacceptable behavior. Fairness, generosity, and loyalty are examples of virtues, while vanity, greed, envy, and anger are considered vices. People's virtues and vices help define their personal value system—the complex scheme of moral values by which they live.

Although nearly everyone would agree that certain behaviors—such as lying and cheating—are wrong, opinions about what constitutes right and wrong behaviors can vary dramatically. For example, attitudes toward **software piracy**—a form of copyright infringement that involves making copies of software or enabling others to access software to which they are not entitled—range from strong opposition to acceptance of the practice as a standard approach to conducting business. According to the Business Software Alliance (BSA), the global rate of software piracy stands at around 42 percent. The piracy rate is nearly 80 percent across the continent of Africa, where many consumers simply cannot afford software licenses and pirated copies are readily available at cut-rate prices.[5]

Individual views of what behavior is moral may be impacted by a person's age, cultural group, ethnic background, religion, life experiences, education, and gender along with many other factors. There is widespread agreement on the immorality of murder, theft, and arson, but other behaviors that are accepted in one culture might be unacceptable in another. Even within the same society, people can have strong disagreements over important moral issues. In the United States, for example, issues such as abortion, stem cell research, the death penalty, same-sex marriage, marijuana usage, and gun control are continuously debated, and people on both sides of these debates feel that their arguments are on solid moral ground. The reality is that the world has many systems of beliefs about what is right and wrong, each with many proponents.

Life is complex, and on occasion, you will encounter a situation in which the ethics of the group to which you belong are in conflict with your morals, as highlighted in the following two examples:

- The ethics of the law profession demand that defense attorneys defend an accused client to the best of their ability, even if they know that the client is guilty of the most heinous and morally objectionable crime one could imagine.
- The ethical standards of the medical profession do not allow a doctor to euthanize a patient, even at the patient's request. However, the doctor may personally believe that the patient has a right, based on the doctor's own morals.

Figure 1-1 illustrates the relationship between ethics and morals and identifies some of the many factors that help define them.

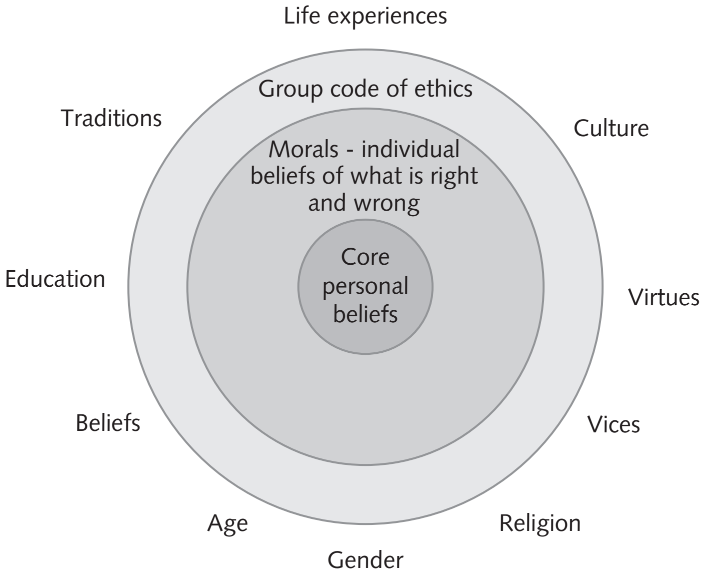


FIGURE 1-1 The relationship between ethics and morals

The Importance of Integrity

A person who acts with **integrity** acts in accordance with a personal code of principles. One approach to acting with integrity is to extend to all people the same respect and consideration that you expect to receive from them. Unfortunately, consistency can be difficult to achieve, particularly when you are in a situation that conflicts with your moral standards. For example, you might believe it is important to do as your employer requests while also believing that you should be fairly compensated for your work. Thus, if your employer insists that, due to budget constraints, you do not report the overtime hours that you have worked, a moral conflict arises. You can do as your employer requests or you can insist on being fairly compensated, but you cannot do both. In this situation, you may be forced to compromise one of your principles and act with an apparent lack of integrity.

Another form of inconsistency emerges if you apply moral standards differently according to the situation or people involved. If you are consistent and act with integrity, you apply the same moral standards in all situations. For example, you might consider it morally acceptable to tell a little white lie to spare a friend some pain or embarrassment, but would you lie to a work colleague or customer about a business issue to avoid unpleasantness? Clearly, many ethical dilemmas are not as simple as right versus wrong but involve choices between right versus right. As an example, for some people it is “right” to protect the Alaskan wildlife from being spoiled and also “right” to find new sources of oil to maintain U.S. oil reserves, but how do they balance these two concerns?

The Difference Between Morals, Ethics, and Laws

Law is a system of rules that tells us what we can and cannot do. Laws are enforced by a set of institutions (the police, courts, law-making bodies). Violation of a law can result in censure, fines, and/or imprisonment. Laws in the United States are made by the various local, state, and federal legislatures. Sometimes the laws of these various jurisdictions are in conflict, creating confusion and uncertainty. In addition, laws are not static; new laws are constantly being introduced and existing laws repealed or modified. As a result, the precise meaning of a particular law may be different in the future from what it is today.

Legal acts are acts that conform to the law. Moral acts conform to what an individual believes to be the right thing to do. Laws can proclaim an act as legal, although many people may consider the act immoral—for example, abortion. Laws may also proclaim an act as illegal, although many people may consider the act moral—for example, using marijuana to relieve stress and nausea for people undergoing chemotherapy treatment for cancer.

Laws raise important and complex issues concerning equality, fairness, and justice, but do not provide a complete guide to ethical behavior. Just because an activity is defined as legal does not mean that it is ethical (see Figure 1-2). As a result, practitioners in many professions subscribe to a code of ethics that states the principles and core values that are essential to their work and, therefore, govern their behavior. The code can become a reference point for helping an individual determine what is legal and what is ethical; however, an individual will also be guided by his or her set of morals.

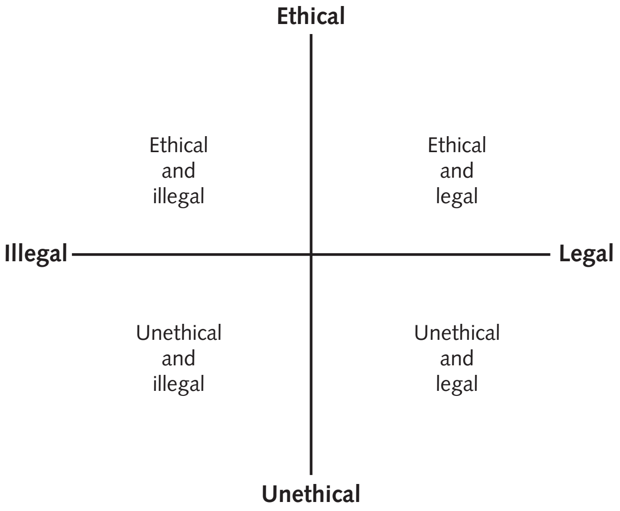


FIGURE 1-2 Legal versus ethical

CRITICAL THINKING EXERCISE: LEGAL VERSUS ETHICAL

Give an example of an action that fits in each of the four quadrants of the legal versus ethical chart shown in Figure 1-2—ethical and legal, ethical and illegal, unethical and illegal, and unethical and legal.

The remainder of this chapter provides an introduction to ethics in the business world. It discusses the importance of ethics in business, outlines what businesses can do to improve their ethics, advises on creating an ethical work environment, and suggests a model for ethical decision making. The chapter concludes with a discussion of ethics as it relates to information technology (IT).

ETHICS IN THE BUSINESS WORLD

Ethics has risen to the top of the business agenda because the risks associated with inappropriate behavior have increased, both in their likelihood and in their potential negative impact. We have seen the collapse and/or bailout of financial institutions such as Bank of America, CitiGroup, Countrywide Financial, Fannie Mae, Freddie Mac, Lehman Brothers, and American International Group (AIG) due to unwise and/or unethical decision making regarding the approval of mortgages, loans, and lines of credit to unqualified individuals and organizations. We have also witnessed numerous corporate officers and senior managers sentenced to prison terms for their unethical behavior, including former investment broker Bernard Madoff, who bilked his clients out of an estimated $65 billion, and Stewart Parnell, former CEO of Peanut Corporation of America, who was sentenced to 28 years in prison for knowingly shipping contaminated food product, resulting in a salmonella outbreak that killed nine people and sickened more than 700.[6,7] Clearly, unethical behavior in the business world can lead to serious negative consequences for both organizations and individuals.

Several trends have increased the likelihood of unethical behavior. First, for many organizations, greater globalization has created a much more complex work environment that spans diverse cultures and societies, making it more difficult to apply principles and codes of ethics consistently. Numerous U.S. companies have moved operations to developing countries, where employees or contractors work in conditions that would not be acceptable in the most developed parts of the world. For example, it was reported in 2016 that employees of the Pegatron factory in China, where the Apple iPhone is produced, are often forced to work excessive amounts of overtime—up to 90 overtime hours per month—while their overall wages have been cut from $1.85 to $1.60 per hour.[8]

Second, in today's challenging and uncertain economic climate, many organizations are finding it more difficult to maintain revenue and profits. Some organizations are sorely tempted to resort to unethical behavior to maintain profits. Tesco, Britain's largest supermarket chain, admitted its first half-year of profits for 2013 were overstated by $400 million.[9] Fiat Chrysler Automobiles admitted its U.S. auto sales were overstated by hundreds of cars each month starting as far back as 2011.[10]

Employees, shareholders, and regulatory agencies are increasingly sensitive to violations of accounting standards, failures to disclose substantial changes in business conditions, nonconformance with required health and safety practices, and production of unsafe or substandard products. Such heightened vigilance raises the risk of financial loss for businesses that do not foster ethical practices or that run afoul of required standards. There is also a risk of criminal and civil lawsuits resulting in fines and/or incarceration for individuals.

A classic example of the many risks associated with unethical decision making can be found in the Enron accounting scandal. In 2000, Enron—a Texas-based energy company—employed over 22,000 people, and it reported an annual revenue of $101 billion. However, in 2001, it was revealed that much of Enron's revenue was the result of deals with limited partnerships, which it controlled. In addition, as a result of actions taken contrary to generally accepted accounting practices (GAAP), many of Enron's debts and losses were not reported in its financial statements. As the accounting scandal unfolded, Enron shares dropped from $90 per share to less than $1 per share, and the company was forced to file for bankruptcy.[11] The Enron case was notorious, but many other corporate scandals have occurred in spite of safeguards enacted as a result of the Enron debacle. Here are just a few examples of lapses in business ethics by employees in IT organizations:

- Volkswagen has admitted that 11 million of its vehicles were equipped with software that was used to cheat on emissions tests. The company is now contending with the fallout.
- Toshiba, the Japanese industrial giant whose diversified products and services include information technology and communications equipment and systems, disclosed that it overstated its earnings over a seven-year period by more than $1.2 billion.
- Amazon has the second highest employee turnover rate of companies in the Fortune 500 and has been criticized by some for creating a high pressure work environment in which bosses' expectations were almost impossible to satisfy and jobs were threatened if illness or other personal issues encroached on work.[12]

It is not unusual for powerful, highly successful individuals to fail to act in morally appropriate ways, as these examples illustrate. Such people are often aggressive in striving for what they want and are used to having privileged access to information, people, and other resources. Furthermore, their success often inflates their belief that they have the ability and the right to manipulate the outcome of any situation. The moral corruption of people in power, which is often facilitated by a tendency for people to look the other way when their leaders act inappropriately has been given the name **Bathsheba syndrome**—a reference to the biblical story of King David, who became corrupted by his power and success.[13] According to the story, David became obsessed with Bathsheba, the wife of one of his generals, and eventually ordered her husband on a mission of certain death so that he could marry Bathsheba.

Even lower-level employees and ordinary individuals can find themselves in the middle of ethical dilemmas, as these examples illustrate:

- Edward Snowden, working as a Dell contractor at the National Security Agency (NSA), copied thousands of classified and unclassified documents that revealed details about the capabilities and scope of operations of the NSA and other foreign intelligence agencies. The documents were then handed over to reporters who published many of the disclosures in the *Guardian* and *Washington Post* newspapers. Snowden felt he acted as a patriot in exposing the behavior of the NSA, which he thought was overreaching and counter to the U.S. Constitution. Some consider him a whistle-blower and a hero, while others see him as a traitor.

- Mark Lillie, a former Takata Corporation engineer, warned the company of the potential deadly consequences of using the propellant ammonium nitrate to inflate its airbags. The use of ammonium nitrate enabled Takata to earn a greater profit than other designs, however, it also resulted in devices that can deploy with too much force, causing them to rupture and shoot metal fragments at motorists. Unfortunately, Lillie was unable to convince management at Takata to choose an alternative design. He eventually left the firm in disagreement over this fatal manufacturing decision. In the United States, at least 10 deaths and more than 100 injuries have been attributed to the flawed devices, and over 100 million cars with Takata inflators have been recalled worldwide.[14,15]

This is just a small sample of the incidents that have led to an increased focus on business ethics within many IT organizations. Table 1-1 identifies the most commonly observed types of misconduct in the workplace.

TABLE 1-1 Most common forms of employee misconduct

Type of employee misconduct	Percentage of surveyed employees observing this behavior in the workplace
Misuse of company time	33
Abusive behavior	21
Lying to employees	20
Company resource abuse	20
Violating company Internet use policies	16
Discrimination	15
Conflicts of interest	15
Inappropriate social networking	14
Health or safety violations	13
Lying to outside stakeholders	12
Stealing	12
Falsifying time reports or hours worked	12

Source: Ethics Resource Center, “2011 National Business Ethics Survey: Workplace Ethics in Transition,” © 2011, https://s3.amazonaws.com/berkley-center/120101NationalBusinessEthicsSurvey2011WorkplaceEthicsinTransition.pdf.

According to the 2013 National Business Ethics Survey, it is managers—those expected to act as role models and enforce discipline—who are responsible for 60 percent of workplace misconduct, as shown in Figure 1-3.[16]

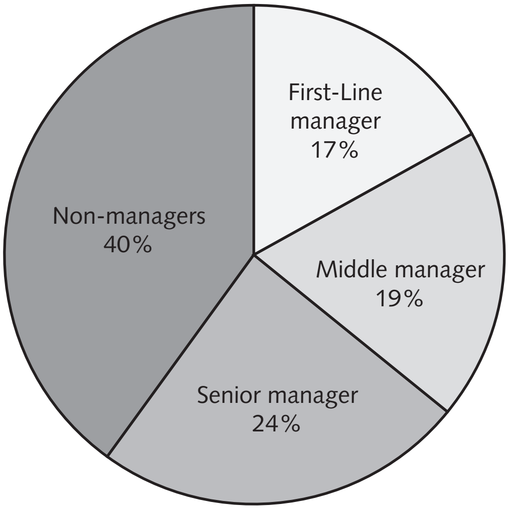


FIGURE 1-3 Who is responsible for instances of misconduct

Source: Ethics Resource Center, "2011 National Business Ethics Survey: Workplace Ethics in Transition," ©2011, https://s3.amazonaws.com/berkley-center/120101NationalBusinessEthicsSurvey2011WorkplaceEthicsinTransition.pdf.

CRITICAL THINKING EXERCISE: CUT TESTING SHORT

You are a new hire at a large software firm and have been working overtime for the last two months trying to complete the final testing of a new software release for the firm's flagship product, which is used by thousands of organizations worldwide. Unfortunately, the software has many bugs and testing has taken weeks longer than expected. This afternoon your boss stopped by and asked you to "sign off" on the completion of your portion of the testing. He explains that the project has gone over budget and is in danger of missing the committed release date for customers. When you object because you feel the software is still buggy, he says not to worry, whatever bugs remain will be fixed in the next release of the software. What do you do?

CORPORATE SOCIAL RESPONSIBILITY

Corporate social responsibility (CSR) is the concept that an organization should act ethically by taking responsibility for the impact of its actions on its shareholders, consumers, employees, community, environment, and suppliers (see Figure 1-4). An organization's approach to CSR can encompass a wide variety of tactics—from donating a portion of net profit to charity to implementing more sustainable business operations or encouraging employee education through tuition reimbursement. Setting CSR goals encourages an organization to achieve higher moral and ethical standards.

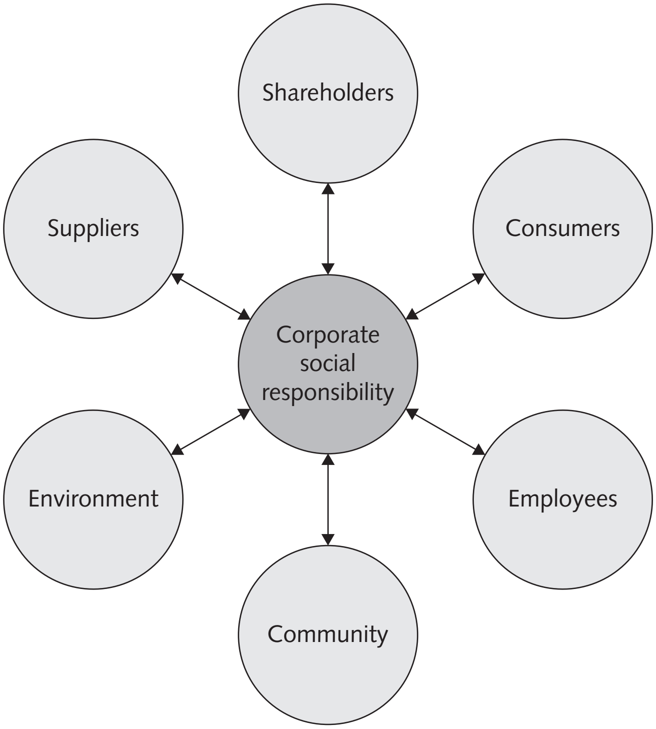


FIGURE 1-4 An organization's program CSR affects its shareholders, consumers, employees, community, environment, and suppliers

Supply chain sustainability is a component of CSR that focuses on developing and maintaining a supply chain that meets the needs of the present without compromising the ability of future generations to meet their needs. Supply chain sustainability takes into account issues such as fair labor practices, energy and resource conservation, human rights, and community responsibility. Many IT equipment manufacturers have made supply chain sustainability a priority, in part, because they must adhere to various European Union directives and regulations—including the Restriction of Hazardous Substances Directive, the Waste Electrical and Electronic Equipment Directive, and the Registration, Evaluation, Authorization, and Restriction of Chemicals (REACH) Regulation—to be permitted to sell their products in the European Union countries. In many cases, meeting supply chain sustainability goals can also lead to lower costs. For example, in fiscal year 2015, Dell launched its closed-loop plastics supply chain and by year end had recycled 2.2 million pounds of those plastics back into new Dell products. In addition, its global takeback program has made Dell the world's largest technology recycler, collecting more than 1.4 billion pounds of e-waste since 2007.[17]

Each organization must decide if CSR is a priority and, if so, what its specific CSR goals are. The pursuit of some CSR goals can lead to increased profits, making it easy for senior company management and stakeholders to support the organization's goals in this arena. However, if striving to meet a specific CSR goal leads to a decrease in profits, senior management may be challenged to modify or drop that CSR goal entirely. For example, most U.S. auto manufacturers have introduced models that run on clean, renewable electric power as part of a corporate responsibility goal of helping to end U.S. dependence on oil. However, Americans have been slow to embrace electric cars, and many manufacturers have had to offer low-interest financing, cash discounts, sales bonuses, and subsidized leases to get the autos off the sales floor. Manufacturers and dealers are struggling to increase profits on the sale of these electric cars, and senior management at the automakers must consider how long they can continue with their current strategies.

Many organizations define a wide range of corporate responsibility areas that are important to them, their customers, and their community. In order for a CSR program to be effective, a senior executive should be placed in charge of corporate responsibility results for each area, with strategic initiatives defined, staffed, and well-funded. Key indicators of progress in these areas should be defined and the results tracked and reported to measure progress.

Table 1-2 shows a summary of the 2015 corporate responsibility report for Intel. An example of one strategic initiative at Intel is its diversity and inclusion initiative launched in early 2015 whose goal is to achieve full representation of women and underrepresented minorities in Intel's workforce by 2020.

TABLE 1-2 Intel Corporate Responsibility Report for 2015

Key performance area	Key performance indicator	2015 value
Financial results and economic impact	Net revenue	$55.4B
	Net income	$11.4B
	Provision for taxes	$2.8B
	Research and development spending	$12.1B
	Capital investments	$7.3B
	Customer survey "Delighted" score	87%
Environmental sustainability	Greenhouse gas emissions (millions of metric tons of CO_2)	2.00
	Energy usage (billions of kWh)	6.4
	Total water withdrawn (billions of gallons)	9.0
	Hazardous waste generated (thousands of tons)/% to landfill	61.6/2
	Nonhazardous waste generated (thousands of tons)/% recycled	80.8/82
Our people	Employees at year end (thousands)	107.3
	Women in global workforce (percent)	25%
	Women on our board of directors at year-end (percent)	18%
	Investment in training (millions of dollars)	$278
	Safety (recordable rate/days away case rate)	0.58/0.11
	Organizational Health Survey scores—"Proud to Work for Intel"	84% (2014)
Social impact	Employee volunteerism rate	41%
	Worldwide charitable giving (dollars in millions)	$90.3
	Charitable giving as a percentage of pre-tax net income	0.6%
Supply chain responsibility	Supplier audits (third-party and Intel-led audits)	121

Source: "2015 Corporate Responsibility Report," Intel, http://csrreportbuilder.intel.com/PDFfiles/CSR-2015_Executive-Summary.pdf, accessed August 10, 2016.

CRITICAL THINKING EXERCISE: ORACLE CSR PROGRAM

Oracle Corporation, a multinational computer technology company with headquarters in Redwood City, California, offers a comprehensive and fully integrated set of cloud applications, platform services, and engineered systems. Oracle has 132,000 employees and more than 420,000 customers, and its software is deployed in more than 145 countries. For fiscal year 2016, the company's total revenue was $37.0 billion, with net income of $8.9 billion. Oracle has set corporate social responsibility goals in the areas of sustainability, education, giving, and volunteering. Develop two goals for each of these areas that you feel would be reasonable for Oracle to achieve. Download the 2016 Oracle Corporate Citizenship Report at *https://www.oracle.com/corporate/citizenship/index.html*. After reviewing the report, comment on the difference between the goals you identified and Oracle's actual programs.

WHY FOSTERING CORPORATE SOCIAL RESPONSIBILITY AND GOOD BUSINESS ETHICS IS IMPORTANT?

Organizations have at least five good reasons to pursue CSR goals and to promote a work environment in which employees are encouraged to act ethically when making business decisions:

- Gaining the goodwill of the community
- Creating an organization that operates consistently
- Fostering good business practices
- Protecting the organization and its employees from legal action
- Avoiding unfavorable publicity

Gaining the Goodwill of the Community

Although organizations exist primarily to earn profits or provide services to customers, they also have some fundamental responsibilities to society. As discussed in the previous section, companies often declare these responsibilities in specific CSR goals.

All successful organizations, including technology firms, recognize that they must attract and maintain loyal customers. Philanthropy is one way in which an organization can demonstrate its values in action and make a positive connection with its stakeholders. (A **stakeholder** is someone who stands to gain or lose, depending on how a particular situation is resolved.) As a result, many organizations initiate or support socially responsible activities, which may include making contributions to charitable organizations and nonprofit institutions, providing benefits for employees in excess of any legal requirements, and devoting organizational resources to initiatives that are more socially desirable than profitable. Here are a few examples of some of the CSR activities supported by major IT organizations:

- Dell Inc. has several initiatives aimed at reducing the amount of natural resources it takes to create and ship its products, cutting the amount of energy it takes its customers to use its products, and curbing the effects its products have on people and the planet.[18]
- Google agreed to invest more than $1.5 billion in renewable energy projects, such as large-scale wind farms and rooftop solar panels.[19]
- IBM created a program to train transitioning service members to become certified as advanced data analysts. The company also launched the P-TECH program to help students from low-income families finish high school and obtain associate degrees. Several graduates of the program have taken entry-level jobs at IBM while continuing to work toward a four-year degree.[20]
- Microsoft made $922 million in technology donations to more than 120,000 nonprofit organizations globally, and its employees contributed $117 million to 20,000 nonprofits through the company's corporate giving program.[21]
- Oracle delivered nearly $5 billion in resources (with a focus on computer science education) to help 2.2 million students in 100 countries become college-and-career ready.[22]
- SAP pledged over $1 billion toward immediate relief efforts, long-term education, and integration projects to assist refugees, and it initiated a program to provide internship opportunities for more than 100 refugees as well as humanitarian assistance.[23]

The goodwill that CSR activities generate can make it easier for corporations to conduct their business. For example, a company known for treating its employees well will find it easier to compete for the top job candidates. On the other hand, businesses that are not socially responsible run the risk of alienating their customer base. A recent study of more than 10,000 shoppers in 10 different countries revealed that more than 90 percent are likely to switch to brands that support a socially responsible cause, given similar price and quality. In addition, 90 percent of the shoppers surveyed would boycott a company if they learned that the firm engaged in socially irresponsible business practices. Indeed, 55 percent of the respondents had already done so in the previous year.[24]

Creating an Organization That Operates Consistently

Organizations develop and abide by values to create an organizational culture and to define a consistent approach for dealing with the needs of their stakeholders—shareholders, employees, customers, suppliers, and the community. Such a consistency ensures that employees know what is expected of them and can employ the organization's values to help them in their decision making. Consistency also means that shareholders, customers, suppliers, and the community know what they can expect of the organization—that it will behave in the future much as it has in the past. It is especially important for multinational or global organizations to present a consistent face to their shareholders, customers, and suppliers, no matter where those stakeholders live or operate their business. Although each company's value system is different, many share the following values:

- Operate with honesty and integrity, staying true to organizational principles
- Operate according to standards of ethical conduct, in words and action
- Treat colleagues, customers, and consumers with respect
- Strive to be the best at what matters most to the organization
- Value diversity
- Make decisions based on facts and principles

Fostering Good Business Practices

In many cases, good ethics can mean good business and improved profits. Companies that produce safe and effective products avoid costly recalls and lawsuits. (The recall of the weight loss drug Fen-Phen cost its maker, Wyeth-Ayerst Laboratories, almost $14 billion in awards to victims, many of whom developed serious health problems as a result of taking the drug.[25]) Companies that provide excellent service retain their customers instead of losing them to competitors. Companies that develop and maintain strong employee relations enjoy lower turnover rates and better employee morale. Suppliers and other business partners often place a priority on working with companies that operate in a fair and ethical manner. All these factors tend to increase revenue and profits while decreasing expenses. As a result, ethical companies tend to be more profitable over the long term than unethical companies.

On the other hand, bad ethics can lead to bad business results. Bad ethics can have a negative impact on employees, many of whom may develop negative attitudes if they perceive a difference between their own values and those stated or implied by an organization's actions. In such an environment, employees may suppress their tendency to act in a manner that seems ethical to them and instead act in a manner that will protect them against anticipated punishment. When such a discrepancy between employee and organizational ethics occurs, it destroys employee commitment to organizational goals and objectives, creates low morale, fosters poor performance, erodes employee involvement in organizational improvement initiatives, and builds indifference to the organization's needs.

Protecting the Organization and Its Employees from Legal Action

In a 1909 ruling (*United States v. New York Central & Hudson River Railroad Co*.), the U.S. Supreme Court established that an employer can be held responsible for the acts of its employees even if the employees act in a manner contrary to corporate policy and their employer's directions.[26] The principle established is called *respondeat superior*, or "let the master answer."

When it was uncovered that employees of Wells Fargo Bank opened over 2 million bogus credit card accounts not authorized by its customers, the bank was fined over $185 million and ordered to pay customers full restitution for any fees or charges they may have incurred. The practice began at least as early as 2011 and was an attempt by thousands of bank employees to achieve their sales targets for cross-selling and be rewarded with higher sales bonuses.[27] Cross-selling is the practice of selling multiple products to the existing customers—savings account, checking account, auto loan, mortgage, credit card, etc. Cross-selling to existing customers is cheaper than locating and selling to brand new customers. It also tends to lock existing customers into your bank.

A coalition of several legal organizations, including the Association of Corporate Counsel, the U.S. Chamber of Commerce, the National Association of Manufacturers, the National Association of Criminal Defense Lawyers, and the New York State Association of Criminal Defense Lawyers, argues that organizations should "be able to escape criminal liability if they have acted as responsible corporate citizens, making strong efforts to prevent and detect misconduct in the workplace."[28] One way to do this is to establish effective ethics and compliance programs. However, some people argue that officers of companies should not be given light sentences if their ethics programs fail to deter criminal activity within their firms.

Avoiding Unfavorable Publicity

The public reputation of a company strongly influences the value of its stock, how consumers regard its products and services, the degree of oversight it receives from government agencies, and the amount of support and cooperation it receives from its business partners. Thus, many organizations are motivated to build a strong ethics program to avoid negative publicity. If an organization is perceived as operating ethically, customers, business partners, shareholders, consumer advocates, financial institutions, and regulatory bodies will usually regard it more favorably.

Prominent ad buyers and marketers are angry with Facebook after finding out that the world's largest online social network service greatly exaggerated the average viewing time of video ads on its platform. This is a key metric used by advertisers in deciding how much to spend on Facebook video versus other video services such as YouTube, Twitter, and TV networks. It turns out that Facebook was not including views of three seconds or less in calculating its average view time, resulting in overestimating viewing time by 60 to 80 percent.[29] Some advertising industry analysts believe that the new viewing time results and bad publicity associated with the incident will be impactful in the future placement of tens of billions of advertising dollars.

CRITICAL THINKING EXERCISE: REGULATING CSR SPENDING

Section 135 of the India Companies Act of 2013 requires companies with net worth, revenue, or net profit above certain established thresholds to spend at least 2 percent of their average net profit of the preceding three years on CSR activities. The act has had a major impact in increasing spending on CSR activities in India. Four of the country's top IT service firms—Tata Consultancy Services Ltd., Wipro Ltd, Infosys Ltd., and Tech Mahindra Ltd.—spent about $96 million on CSR activities within India during the first year this rule was in effect. That is 4.7 times the amount they spent on CSR initiatives the previous year, when the rule was not yet in effect. Collectively, these four firms generate over $35 billion in annual revenue.

The companies' CSR activities include efforts to eradicate hunger, poverty, and disease; promote education, gender equality, and women's empowerment; reduce child mortality; improve healthcare and sanitation; and provide safe drinking water.[30]

Does mandated CSR spending by all organizations within a particular country or market reduce the benefits an individual organization can expect to gain from its CSR programs? Do you think the United States should pass a law similar to Section 135 of the India Companies Act? Why or why not? If so, should the amount required for CSR spending be higher than two percent of average net profit?

HOW ORGANIZATIONS CAN IMPROVE THEIR ETHICS

Research by the Ethics Resource Center (ERC) found that 86 percent of the employees in companies with a well-implemented ethics and compliance program are likely to perceive a strong ethical culture within the company, while less than 25 percent of employees in companies with little to no program are likely to perceive a culture that promotes integrity in the workplace. A well-implemented ethics and compliance program and a strong ethical culture can, in turn, lead to less pressure on employees to misbehave and a decrease in observed misconduct. It also creates an environment in which employees are more comfortable reporting instances of misconduct, partly because there is less fear of potential retaliation by management against reporters (for example, reduced hours, transfer to less desirable jobs, and delays in promotions). See Figure 1-5.[31]

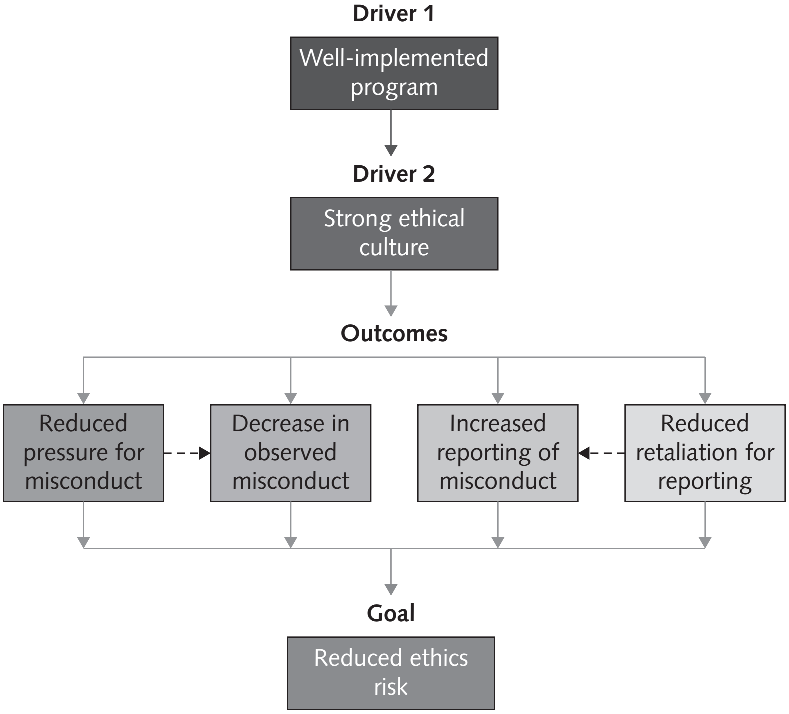

Driver 1
Well-implemented program
Driver 2
Strong ethical culture
Outcomes
Reduced pressure for misconduct
Decrease in observed misconduct
Increased reporting of misconduct
Reduced retaliation for reporting
Goal
Reduced ethics risk

FIGURE 1-5 Reducing the risk of unethical behavior

Source: Ethics Resource Center, "2011 National Business Ethics Survey: Workplace Ethics in Transition," © 2011, https://s3.amazonaws.com/berkley-center/120101NationalBusinessEthicsSurvey2011WorkplaceEthicsinTransition.pdf.

The Ethics Resource Center has defined the following characteristics of a successful ethics program:

- Employees are willing to seek advice about ethics-related issues.
- Employees feel prepared to handle situations that could lead to misconduct.

- Employees are rewarded for ethical behavior.
- The organization does not reward success obtained through questionable means.
- Employees feel positively about their company.

The 2013 National Business Ethics Survey found evidence of continuing improvement in ethics in the workplace, as summarized in Table 1-3. The survey results indicate that fewer employees witnessed misconduct on the job, but when they did, they were more willing to report it. They also show that there is a decrease in the percentage of employees who felt pressure to commit an unethical act and who feel their organization has a weak ethics culture.

In addition to reporting on some positive trends in workplace ethics, however, the survey also highlighted some areas of concern. For instance, about 21 percent of those who reported misconduct stated that they suffered from some sort of retribution from their supervisor or negative reaction from their coworkers; that amounts to an estimated 6.2 million American workers who have faced a backlash for reporting misconduct.[32]

TABLE 1-3 Conclusions from the 2013 National Business Ethics Survey

Finding	2007 Survey results	2009 Survey results	2011 Survey results	2013 Survey results
Percentage of employees who said they witnessed a violation of the law or ethics standards on the job	56	49	45	41
Percentage of employees who said they reported misconduct when they saw it	58	63	65	63
Percentage of employees who felt pressure to commit an ethics violation	10	8	13	9
Percentage of employees who say their business has a weak ethics culture	39	35	42	36

Source: Ethics and Compliance Initiative, "National Business Ethics Survey 2013," www.ethics.org/eci/research/eci-research/nbes/nbes-reports/nbes-2013.

The risk of unethical behavior is increasing, so improving business ethics is becoming more important for all companies. The following sections explain some of the actions corporations can take to improve business ethics.

Appoint a Corporate Ethics Officer

A **corporate ethics officer** (also called a **corporate compliance officer**) provides an organization with vision and leadership in the area of business conduct. This individual "aligns the practices of a workplace with the stated ethics and beliefs of that workplace, holding people accountable to ethical standards."[33]

Organizations send a clear message to employees about the importance of ethics and compliance in their decision about who will be in charge of the effort and to whom that individual will report. Ideally, the corporate ethics officer should be a well-respected, senior-level manager who reports directly to the CEO. Ethics officers come from diverse backgrounds, such as legal staff, human resources, finance, auditing, security, or line operations.

Not surprisingly, a rapid increase in the appointment of corporate ethics officers typically follows the revelation of a major business scandal. The first flurry of appointments in the United States began following a series of defense-contracting scandals during the administration of Ronald Reagan in the late 1980s—when firms used bribes to gain inside information that they could use to improve their contract bids. A second spike in appointments came in the early 1990s, following new federal sentencing guidelines that stated that "companies with effective compliance and ethics programs could receive preferential treatment during prosecutions for white-collar crimes."[34] A third surge followed the myriad accounting scandals of the early 2000s. Yet another increase in appointments followed in the aftermath of the mortgage loan scandals uncovered beginning in 2008.

The ethics officer position has its critics. Many are concerned that if one person is appointed head of ethics, others in the organization may think they have no responsibility in this area. On the other hand, Odell Guyton—a long-time director of compliance at Microsoft—feels a point person for ethics is necessary, otherwise, "how are you going to make sure it's being done, when people have other core responsibilities? That doesn't mean it's on the shoulders of the compliance person alone."[35]

Typically, the ethics officer tries to establish an environment that encourages ethical decision making through the actions described in this chapter. Specific responsibilities include the following:

- Responsibility for compliance—that is, ensuring that ethical procedures are put into place and consistently adhered to throughout the organization
- Responsibility for creating and maintaining the ethics culture envisioned by the highest level of corporate authority
- Responsibility for being a key knowledge and contact person on issues relating to corporate ethics and principles[36]

Of course, simply naming a corporate ethics officer does not automatically improve an organization's ethics; hard work and effort are required to establish and provide ongoing support for an organizational ethics program.

Require the Board of Directors to Set and Model High Ethical Standards

The board of directors is responsible for the careful and responsible management of an organization. In a for-profit organization, the board's primary objective is to oversee the organization's business activities and management for the benefit of all stakeholders, including shareholders, employees, customers, suppliers, and the community. In a nonprofit organization, the board reports to a different set of stakeholders—in particular, the local community that the nonprofit serves.

A board of directors fulfills some of its responsibilities directly and assigns others to various committees. The board is not normally responsible for day-to-day management and operations; these responsibilities are delegated to the organization's management team. However, the board is responsible for supervising the management team.

Board members are expected to conduct themselves according to the highest standards for personal and professional integrity while setting the standard for company-wide ethical conduct and ensuring compliance with laws and regulations. Employees will "get the message" if board members set an example of high-level ethical behavior. If they don't set a good example, employees will get that message as well. Importantly, board members must create an environment in which employees feel they can seek advice about appropriate business conduct, raise issues, and report misconduct through appropriate channels.

The board of directors must set an example of high-level ethical behavior and may need intervention in order to stop unethical behavior, as illustrated by a recent ethics scandal at the Wounded Warrior Project (WWP), a charity and veterans service nonprofit. In 2016, the CEO and COO of WWP were fired by the organization's board of directors over allegations by many current and former employees regarding ineffective and wasteful spending of the more than $372 million the organization received in 2015. The nonprofit spent over 40 percent of its funds on overhead—including luxurious employee retreats and first-class airfare, while creating programs for veterans that were effective for marketing purposes but often failed to address the real needs of veterans.[37] Several months after the scandal became public, the WWP board of directors hired a new CEO who ultimately fired more than half of the nonprofit's executives, closed several offices, and redirected millions of dollars in spending to programs, including those that provide mental healthcare services, which more directly serve veterans.[38]

Establish a Corporate Code of Ethics

A **code of ethics** is a statement that highlights an organization's key ethical issues and identifies the overarching values and principles that are important to the organization and its decision making. Codes of ethics frequently include a set of formal, written statements about the purpose of an organization, its values, and the principles that should guide its employees' actions. An organization's code of ethics applies to its directors, officers, and employees, and it should focus employees on areas of ethical risk relating to their role in the organization, offer guidance to help them recognize and deal with ethical issues, and provide mechanisms for reporting unethical conduct and fostering a culture of honesty and accountability within the organization. An effective code of ethics helps ensure that employees abide by the law, follow necessary regulations, and behave in an ethical manner.

A code of ethics cannot gain company-wide acceptance unless it is developed with employee participation and fully endorsed by the organization's leadership. It must also be easily accessible by employees, shareholders, business partners, and the public. The code of ethics must continually be applied to a company's decision making and emphasized as an important part of its culture. Breaches in the code of ethics must be identified and dealt with appropriately so the code's relevance is not undermined.

Each year, *Corporate Responsibility* magazine rates publicly held U.S. companies, using a statistical analysis of corporate ethical performance in several categories. (For 2016, the categories were environment, climate change, human rights, employee relations, corporate governance, philanthropy and community support, and financial performance.) Intel Corporation, the world's largest chip maker, has been ranked in the top 25 every year since the list began in 2000, and was ranked second in 2016.[39] As such, Intel is recognized as one of the most ethical companies in the IT industry. A summary of Intel's code of ethics is provided below.

Intel's Code of Conduct

Intel's Code of Conduct (see Figure 1-6) applies to all employees and sets expectations for Intel Corporation and its subsidiaries as well as its nonemployee members of the Board of Directors regarding their Intel-related activities. The Code of Conduct also applies to independent contractors, consultants, suppliers, and others who do business with Intel. Each employee is responsible for reading, understanding, and following the Code. Employees who violate the Code are subject to discipline, up to and including termination of employment. Anyone who violates the law may also be subject to civil and criminal penalties.

Intel Code of Conduct Principles

The code affirms Intel's five principles of conduct:

1. Conduct business with honesty and integrity.
2. Follow the letter and spirit of the law.
3. Treat each other fairly.
4. Act in the best interests of Intel and avoid conflicts of interest.
5. Protect the company's assets and reputation

FIGURE 1-6 Intel Code of Conduct Principles

Source: "Intel Code of Conduct," Intel, http://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/policy-code-conduct-corporate-information.pdf, accessed August 10, 2016.

Conduct Social Audits

An increasing number of organizations conduct regular social audits of their policies and practices. In a **social audit**, an organization reviews how well it is meeting its ethical and social responsibility goals and communicates its new goals for the upcoming year. This information is shared with employees, shareholders, investors, market analysts, customers, suppliers, government agencies, and the communities in which the organization operates.

In an ongoing effort to engrain socially responsible business behavior into all business activities, key Dell suppliers undergo a review of their social and environmental progress on a quarterly basis. These reviews include audit performance data, assessment of policy compliance and specific implementation plans for suppliers' own programs for compliance, and environmental stewardship.[40]

Require Employees to Take Ethics Training

The ancient Greek philosophers believed that personal convictions about right and wrong behavior could be improved through education. Today, most psychologists agree with them. Lawrence Kohlberg, the late Harvard psychologist, found that many factors stimulate a person's moral development, but one of the most crucial is education. Other researchers have repeatedly supported the idea that people can continue their moral development through further education, such as working through case studies and examining contemporary issues.

Thus, an organization's code of ethics must be promoted and continually communicated within the organization, from the top to the bottom. Organizations can do this by showing the employees examples of how to apply the code of ethics in real life. One approach is through a comprehensive ethics education program that encourages employees to act responsibly and ethically. Such programs are often presented in small workshop formats in which employees apply the organization's code of ethics to hypothetical but realistic case studies. Employees may also be given examples of recent company decisions based on principles from the code of ethics.

A critical goal of such training is to increase the percentage of employees who report incidents of misconduct; thus, employees must be shown effective ways of reporting such incidents. In addition, they must be reassured that such feedback will be acted on and that they will not be subjected to retaliation.

In its 2013 National Business Ethics Survey, the Ethics Resource Center reported that 81 percent of the surveyed organizations provide ethics training.[41] At IBM, for example, employees around the world take part in the firm's online Business Conduct Guidelines course and certification. This training is available in two dozen languages and presents real-world scenarios that employees may face when conducting business. In addition, senior IBM business leaders sponsor integrity summits that emphasize the role of leaders in creating an ethical culture. The summits also help IBM employees to identify key compliance risks along with specific actions that can mitigate these risks. In addition, IBM provides online ethics and integrity training to almost 20,000 employees of IBM's partners and suppliers around the world.[42]

Formal ethics training not only makes employees more aware of a company's code of ethics and how to apply it but also demonstrates that the company intends to operate in an ethical manner. The existence of formal training programs can also reduce a company's liability in the event of legal action.

Include Ethical Criteria in Employee Appraisals

Managers can help employees to meet performance expectations by monitoring employee behavior and providing feedback; increasingly, managers are including ethical conduct as part of an employee's performance appraisal. Those that do so base a portion of their employees' performance evaluations on treating others fairly and with respect; operating effectively in a multicultural environment; accepting personal accountability for meeting business needs; continually developing others and themselves; and operating openly and honestly with suppliers, customers, and other employees. These factors are considered along with the more traditional criteria used in performance appraisals, such as an employee's overall contribution to moving the business ahead, successful completion of projects and tasks, and maintenance of good customer relations. In a recent survey, about two-thirds of organizations reported that they include ethical conduct as a performance measure in employee evaluations.[43]

Create an Ethical Work Environment

Most employees want to perform their jobs successfully and ethically, but good employees sometimes make bad ethical choices. Employees in highly competitive workplaces often feel pressure from aggressive competitors, cutthroat suppliers, unrealistic budgets, unforgiving quotas, tight deadlines, and bonus incentives. Employees may also be encouraged to do "whatever it takes" to get the job done. In such environments, some employees may feel pressure to engage in unethical conduct to meet management's expectations, especially if the organization has no corporate code of ethics and no strong examples of senior management practicing ethical behavior.

The most important influence on how employees act is their perception of their immediate boss's expectations. If the boss sets the expectation that compliance failures and ethical lapses will not be tolerated, then employees will be less likely to fail.

The following list includes several examples of how managerial behavior can encourage unethical employee behavior:

- A manager sets and holds people accountable to meet "stretch" goals, quotas, and budgets, causing employees to think, "My boss wants results, not excuses, so I have to cut corners to meet the goals my boss has set."
- A manager fails to provide a corporate code of ethics and operating principles to make decisions, so employees think, "Because the company has not established any guidelines, I don't think my conduct is really wrong or illegal."
- A manager fails to act in an ethical manner and instead sets a poor example for others to follow, so employees think, "I have seen other successful people take unethical actions and not suffer negative repercussions."
- Managers fail to hold people accountable for unethical actions, so employees think, "No one will ever know the difference, and if they do, so what?"
- Managers put a three-inch-thick binder entitled "Corporate Business Ethics, Policies, and Procedures" on the desks of new employees and tell them to "read it when you have time and sign the attached form that says you read and understand the corporate policy." Employees think, "This is overwhelming. Can't they just give me the essentials? I can never absorb all this."

Table 1-4 provides a manager's checklist for establishing an ethical workplace. The preferred answer to each question is *yes*.

Employees must have a knowledgeable resource with whom they can discuss perceived unethical practices. For example, Intel expects employees to report suspected violations of its code of conduct to a manager, the Legal or Internal Audit Departments, or a business unit's legal counsel. Employees can also report violations anonymously through an internal website dedicated to ethics. Senior management at Intel has made it clear that any employee can report suspected violations of corporate business principles without fear of reprisal or retaliation.

TABLE 1-4 Manager's checklist for establishing an ethical work environment

Question	Yes	No
Does your organization have a code of ethics?		
Do employees know how and to whom to report any infractions of the code of ethics?		
Do employees feel that they can report violations of the code of ethics safely and without fear of retaliation?		
Do employees feel that action will be taken against those who violate the code of ethics?		
Do senior managers set an example by communicating the code of ethics and using it in their own decision making?		
Do managers evaluate and provide feedback to employees on how they operate with respect to the values and principles in the code of ethics?		
Are employees aware of sanctions for breaching the code of ethics?		
Do employees use the code of ethics in their decision making?		

CRITICAL THINKING EXERCISE: HOW DOES YOUR EMPLOYER RATE?

Audit your most recent place of employment using the checklist in Table 1-4. Assign one point for each "yes" answer. What is your employer's score? What changes would you like to see made within your organization to improve that score?

INCLUDING ETHICAL CONSIDERATIONS IN DECISION MAKING

We are all faced with difficult decisions in our work and in our personal life. Most of us have developed a decision-making process that we execute automatically, without thinking about the steps we go through. For many of us, the process generally follows the steps outlined in Figure 1-7.

The following sections discuss this decision-making process further and point out where and how ethical considerations need to be brought into the process.

Develop Problem Statement

A **problem statement** is a clear, concise description of the issue that needs to be addressed. A good problem statement answers the following questions: What do people observe that causes them to think there is a problem? Who is directly affected by the problem? Is anyone else affected? How often does the problem occur? What is the impact of the problem? How serious is the problem?

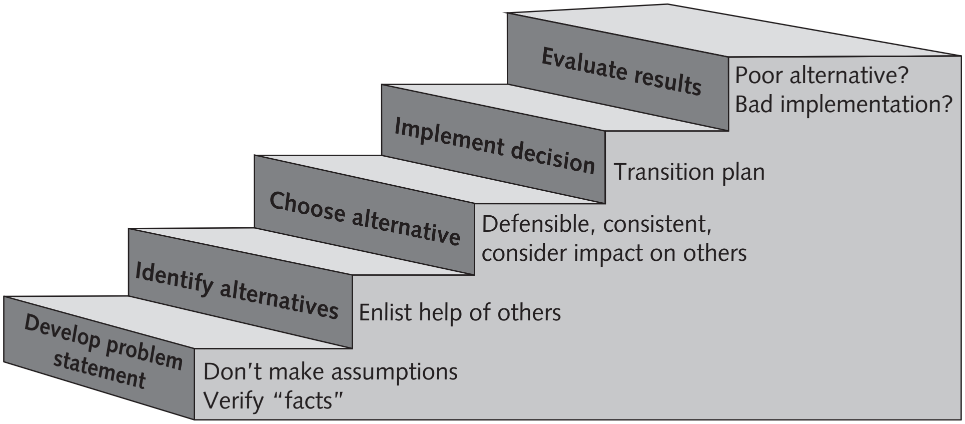


FIGURE 1-7 A five-step ethical decision-making process

Development of a problem statement is the most critical step in the decision-making process. Without a clear statement of the problem or the decision to be made, it is useless to proceed. If the problem is stated incorrectly, the chances of solving the real problem are greatly diminished. The following list includes one example of a good problem statement as well as two examples of poor problem statements:

- Good problem statement: Our product supply organization is continually running out of stock of finished products, creating an out-of-stock situation on over 15 percent of our customer orders, resulting in over $300,000 in lost sales per month.
- Poor problem statement: We need to implement a new inventory control system. (This is a possible solution, not a problem statement. Pursuing this course of action will surely be expensive and time consuming and, may or may not, solve the underlying problem.)
- Poor problem statement: We need to install cameras and monitoring equipment to put an end to theft of finished product in the warehouse. (Again, this is a possible solution, not a problem statement. And are there sufficient facts to support the hypothesis of theft in the warehouse?)

You must gather and analyze facts to develop a good problem statement. Seek information and opinions from a variety of people to broaden your frame of reference. During this process, you must be extremely careful not to make assumptions about the situation and carefully check key facts for validity. Simple situations can sometimes turn into complex controversies because no one takes the time to gather and analyze the real facts.

Identify Alternatives

During this stage of decision making, it is ideal to enlist the help of others, including stakeholders, to identify several alternative solutions to the problem. Brainstorming with others will increase your chances of identifying a broad range of alternatives and determining the best solution. On the other hand, there may be times when it is inappropriate to involve others in solving a problem that you are not at liberty to discuss. In providing participants information about the problem to be solved, offer just the facts, without your opinion, so you don't influence others to accept your solution.

During any brainstorming process, try not to be critical of ideas, as any negative criticism will tend to shut down the discussion, and the flow of ideas will dry up. Simply write down the ideas as they are suggested and ask questions only to gain a clearer understanding of the proposed solution.

Choose Alternative

Once a set of alternatives has been identified, the group must evaluate them based on numerous criteria, such as effectiveness of addressing the issue, the extent of risk associated with each alternative, cost, and time to implement. An alternative that sounds attractive but that is not feasible will not help solve the problem.

As part of the evaluation process, weigh various laws, guidelines, and principles that may apply. You certainly do not want to violate a law that can lead to a fine or imprisonment for yourself or others. Do any corporate policies or guidelines apply? Does the organizational code of ethics offer guidance? Do any of your own morals apply?

Consider the likely consequences of each alternative from several perspectives: What is the impact on you, your organization, other stakeholders (including your suppliers and customers), and the environment? Does this alternative do less harm than other alternatives?

The alternative selected should be ethically and legally defensible to a collection of your coworkers, peers, and your profession's governing body of ethics; be consistent with the organization's policies and code of ethics; take into account the impact on others; and, of course, provide a good solution to the problem.

Implement the Decision

Once an alternative is selected, it should be implemented in an efficient, effective, and timely manner. This is often much easier said than done, because people tend to resist change. In fact, the bigger the change, the greater is the resistance to it. Communication is the key to helping people accept a change. It is imperative that someone whom the stakeholders trust and respect answer the following questions:

- Why are we doing this?
- What is wrong with the current way we do things?
- What are the benefits of the new way for you?

A transition plan must be defined to explain to people how they will move from the old way of doing things to the new way. It is essential that the transition be seen as relatively easy and pain free. It may be necessary to train the people affected, provide incentives for making the change in a successful fashion, and modify the reward system to encourage new behaviors consistent with the change.

Evaluate the Results

After the solution to the problem has been implemented, monitor the results to see if the desired effect was achieved and observe its impact on the organization and the various stakeholders. Were the success criteria fully met? Were there any unintended consequences? This evaluation may indicate that further refinements are needed. If so, return to the problem development step, refine the problem statement as necessary, and work through the process again.

On the other hand, the proper alternative may have been selected, but it was implemented in a poor fashion so the desired results were not achieved. This may require redoing some of the implementation steps.

CRITICAL THINKING EXERCISE: AN OVERWHELMED EMPLOYEE

You are the customer support manager for a small software manufacturer. The newest addition to your 10-person team is Elliot, a recent college computer science graduate. She is a little overwhelmed by the volume of calls, but is learning quickly and doing her best to keep up. Today, over lunch, one of the other members of your team informed you that she overheard a phone conversation in which it sounded like Elliot was talking with a headhunter and expressing unhappiness with her current situation. You're shocked and alarmed. You had no idea she was unhappy, and your team desperately needs her help to handle the onslaught of calls generated by the newest release of software. If you're going to lose her, you'll need to find a replacement quickly. Should you confront Elliot and demand to know her intentions? Should you avoid any confrontation and simply begin seeking her replacement? Is some other action appropriate? Follow the five-step process for ethical decision making to decide what your next steps should be.

ETHICS IN INFORMATION TECHNOLOGY

The growth of the Internet and social networks; the ability to capture, store, and analyze vast amounts of personal data; and a greater reliance on information systems in all aspects of life have increased the risk that information technology will be used unethically. In the midst of the many IT breakthroughs in recent years, the importance of ethics and human values has been underemphasized—with a range of consequences. Here are some examples that raise public concern about the ethical use of information technology:

- Governments around the world have implemented various systems that enable the surveillance of their citizens and are struggling to achieve the proper balance between privacy and security.
- Many employees have their email and Internet access monitored while at work, as employers struggle to balance their need to manage important company assets and work time with employees' desire for privacy and self-direction.
- Millions of people have downloaded music and movies at no charge and in apparent violation of copyright laws at tremendous expense to the owners of those copyrights.
- Organizations contact millions of people worldwide through unsolicited email and text messages in an extremely low cost, but intrusive marketing approach.

- Hackers break into databases of financial and retail institutions to steal customer information and then use it to commit identity theft—opening new accounts and charging purchases to unsuspecting victims.
- Students around the world have been caught downloading material from the web and plagiarizing content for their term papers.
- Websites plant cookies or spyware on visitors' hard drives to track their online purchases and activities.

This book is based on two fundamental tenets. First, the general public needs to develop a better understanding of the critical importance of ethics as it applies to IT; currently, too much emphasis is placed on technical issues. IT has a profound effect on society, and IT professionals and end users need to recognize this fact when they implement technology and formulate policies that will have legal ramifications and affect the well-being of millions of consumers.

The second tenet on which this book is based is that important business-technology decisions with strong ethical implications are too often left to the technical experts to decide (for example, what data to gather about customers, where to store it, how to use it, and what level of security to employ to protect it). General business managers must assume greater responsibility for such decisions, but to do so they must be able to make broad-minded, objective decisions based on technical savvy, business know-how, and high ethical standards. They must also try to create a working environment in which ethical dilemmas can be discussed openly, objectively, and constructively.

Thus, the goals of this text are to educate people about the tremendous impact of ethical issues in the successful and secure use of information technology; to motivate people to recognize these issues when making business decisions; and to provide tools, approaches, and useful insights for making ethical decisions.

CRITICAL THINKING EXERCISE: CIO SURPRISES CFO

You are the Chief Financial Officer (CFO) of a midsized manufacturing firm with annual revenue exceeding $100 million. You have heard nothing but positive comments about the new Chief Information Officer (CIO) you hired three months ago. As you listen to her outline what needs to be done to improve the firm's computer security, you are impressed with her energy, enthusiasm, and presentation skills. However, your jaw drops when she states that the total cost of the proposed computer security improvements will be $250,000. This seems like a lot of money for security, given that your firm has had no major incident. Several other items in the budget will either have to be dropped or trimmed back to accommodate such an expenditure. In addition, the $250,000 is above your spending authorization and will require approval by the CEO. This will require you to defend the expenditure, and you are not sure how to do this. As you look around the conference room, you can see that other members of your staff are just as surprised as you. What serious mistake has the CIO made and how could this have been avoided?

Summary

What is ethics?

- Ethics is a code of behavior that is defined by the group to which an individual belongs.
- Morals are the personal principles upon which an individual bases his or her decisions about what is right and what is wrong.
- A person who acts with integrity acts in accordance with a personal code of principles.
- Law is a system of rules that tells us what we can and cannot do. Laws are enforced by a set of institutions (the police, courts, and law-making bodies).
- A code of ethics states the principles and core values that are essential to one's work.
- Just because an activity is defined as legal does not mean that it is ethical.

What trends have increased the likelihood of an unethical behavior?

- Globalization has created a much more complex work environment, making it more difficult to apply principles and codes of ethics consistently.
- Organizations may be tempted to resort to unethical behavior to maintain profits in today's more challenging and uncertain economic climate.
- It is not unusual for powerful, highly successful individuals to fail to act in morally appropriate ways as such people are often aggressive in striving for what they want and are used to having privileged access to information, people, and other resources. Furthermore, their success often inflates their belief that they have the ability and the right to manipulate the outcome of any situation.

What is corporate social responsibility, and why is fostering good business ethics important?

- Corporate social responsibility is the concept that an organization should act ethically by taking responsibility for the impact of its actions on its shareholders, consumers, employees, community, environment, and suppliers.
- Supply chain sustainability is a component of CSR that focuses on developing and maintaining a supply chain that meets the needs of the present without compromising the ability of future generations to meet their needs.
- Each organization must decide if CSR is a priority, and if so, what its specific CSR goals are.
- Organizations have five good reasons for pursuing CSR goals and promoting a work environment in which they encourage employees to act ethically: (1) to gain the goodwill of the community, (2) to create an organization that operates consistently, (3) to foster good business practices, (4) to protect the organization and its employees from legal action, and (5) to avoid unfavorable publicity.

What measures can organizations take to improve their business ethics?

- An organization can take several actions to improve its business ethics including: appointing a corporate ethics officer, requiring its board of directors to set and model high ethical standards, establish a corporate code of ethics, conduct social audits, require employees to take ethics training, include ethical criteria in employee appraisals, and create an ethical work environment.

How can you include ethical considerations in your decision making?

- Often, people employ a simple decision-making model that includes these steps: (1) define the problem, (2) identify alternatives, (3) choose an alternative, (4) implement the decision, and (5) monitor the results.
- You can incorporate ethical considerations into decision making by identifying and involving the stakeholders; weighing various laws, guidelines, and principles—including the organization's code of ethics—that may apply; and considering the impact of the decision on you, your organization, stakeholders, your customers and suppliers, and the environment.

What trends have increased the risk that information technology will be used in an unethical manner?

- The growth of the Internet and social networks; the ability to capture, store, and analyze vast amounts of personal data; and a greater reliance on information systems in all aspects of life have increased the risk that information technology will be used unethically.
- In the midst of the many IT breakthroughs in recent years, the importance of ethics and human values has been underemphasized—with a range of consequences.

Key Terms

Bathsheba syndrome
code of ethics
corporate compliance officer
corporate ethics officer
corporate social responsibility (CSR)
ethics
integrity
law
morals
problem statement
social audit
software piracy
supply chain sustainability
stakeholder
vice
virtue

Self-Assessment Questions

What is ethics?

1. The term ____________ describes the standards or codes of behavior expected of an individual by a group to which the individual belongs.
   a. morals
   b. ethics
   c. virtues
   d. integrity

2. ______________ is/are one's personal beliefs about what is right and wrong.
   a. Virtues and vices
   b. Ethics
   c. Morals
   d. Code of ethics
3. Laws provide a complete guide to ethical behavior. True or False?

What trends have increased the likelihood of an unethical behavior?

4. The moral corruption of people in power has been given the name ______________.
5. According to the Ethics Resource Center, which of the following is the most commonly observed form of employee misconduct?
   a. Lying to employees
   b. Abusive behavior
   c. Inappropriate social networking
   d. Misuse of company time
6. Nonmanagers are responsible for what percent of instances of reported misconduct?
   a. Roughly 25 percent
   b. Over 50 percent
   c. About 40 percent
   d. Less than 33 percent

What is corporate social responsibility, and why is fostering good business ethics important?

7. The goodwill that CSR activities generate can make it easier for corporations to conduct their business but is unlikely to affect the profitability of the firm. True or False?
8. If an employee acts in a manner contrary to corporate policy and their employee's directions, the employer cannot be held responsible for these actions. True or False?

What measures can organizations take to improve their business ethics?

9. Approximately how many U.S. workers have reported worker or manager misconduct and then suffered some sort of retribution from their supervisor or negative reactions from their coworkers?
   a. Less than 5.5 million
   b. Over 10 million
   c. Some 6.2 million
   d. About 8.7 million

10. A statement that highlights an organization's key ethical issues and identifies the overarching values and principles that are important to the organization and its decision making.
    a. Integrity statement
    b. Code of ethics
    c. Mission statement
    d. Vision statement
11. Which of the following is *not* a key goal of employee ethics training?
    a. Increase the percentage of employees who report incidents of misconduct.
    b. Make employees more aware of the company's code of ethics and how to apply it.
    c. Become familiar with various philosophers and how they dealt with ethical issues.
    d. Reduce the company's liability in the event of legal action.

How can you include ethical considerations in your decision making?

12. Identifying the stakeholders and their positions on an issue is a part of which decision-making step?
    a. Define the problem
    b. Review the applicable guidelines, policies, and laws
    c. Identify and evaluate options
    d. Choose the best option
13. If you find yourself rationalizing a decision with the statement "Well, our competitors are doing something far worse"—what action should you *not* take?
    a. Drop this option, and implement the same policy as your competitors.
    b. Reconsider your options.
    c. Realize you are about to make a decision that you will find difficult to justify to others.
    d. Seek input and advice from others.

What trends have increased the risk that information technology will be used in an unethical manner?

14. Important decisions with strong ethical implications are too often left to the technical experts; general business managers must assume greater responsibility for these decisions. True or False?

Self-Assessment Answers

1. c.; 2. c.; 3. False; 4. Bathsheba syndrome; 5. d.; 6. c.; 7. False; 8. False; 9. c.; 10. b.; 11. c.; 12. a.; 13. a.; 14. True

Discussion Questions

1. What does it mean for an organization to act ethically? How can one evaluate whether this is the case?
2. Identify two important life experiences that helped you define your own set of morals.
3. In ethics, a slippery slope begins when one small unethical action is rationalized by the perpetrator as innocuous because nobody really got hurt or because everybody else does it. This rationalization process, called moral disengagement, can lead people to slip into a pattern of bad behavior that becomes difficult to stop. Embezzler Bernie Madoff admitted to starting by stealing a few hundred and then a few thousand from investors. When he got comfortable with that, it eventually ballooned into something really big—he ultimately stole $85 billion from his investors. Can you provide an example of when you or someone you know was tempted to succumb to the slippery slope?
4. It is easy to say that an organization should hire, reward, and dismiss employees based on their character as well as their knowledge and skill, but how could such a policy be implemented?
5. The Ethics Resource Center identified five characteristics of a successful ethics program. Suggest a sixth characteristic, and defend your choice. Which characteristic do you think is the most important and why?
6. It is a common practice for managers to hold people accountable to meet “stretch” goals, quotas, and budgets. Can this be done in a way that does not encourage unethical behavior on the part of employees? Defend your response.
7. Hypothesis: It is easier to establish an ethical work environment in a nonprofit organization than in a for-profit organization. Provide three facts or opinions that support this hypothesis. Provide three facts or opinions that refute the hypothesis.
8. Do you believe that software manufacturers should be tolerant of the practice of software piracy in third-world countries to allow these countries an opportunity to move more quickly into the information age? Why or why not?
9. Comment on the efforts of your employer to promote a work environment in which employees are encouraged to act ethically.
10. Do you believe that the senior managers and executives of an organization should be able to escape criminal liability for the acts of a few of its employees if the organization has a strong corporate social responsibility program focused on protecting the environment, contributing to charitable causes, hiring and promoting women, and treating customers and suppliers fairly? Why or why not?

What Would You Do?

Use the five-step decision-making process discussed in the chapter to analyze the following situations and recommend a course of action.

1. Employers typically focus on two areas in reviewing job candidates—experience and knowledge. As a member of your organization’s human resources group, you have been

thinking about how the recruiting process could be modified to include character as a third area of review. Candidates would be screened based on their honesty, integrity, and courage to do what is right. You have a meeting with your immediate manager coming up and wonder if you should broach this subject with her. If so, you need to be prepared to explain why you think this is important and to offer examples of how such a screening program could be accomplished.

2. You are currently being considered for a major promotion within your company to vice president of marketing. In your current position as manager of advertising, you supervise five managers and two hourly workers. As part of the annual salary review process, you have been given the flexibility to grant your employees an average 3 percent annual salary increase; however, you are strongly considering a lower amount. This would ensure that your department's expenses stay under budget and would send the message that you are able to control costs. What factors do you need to consider in making this decision? How would you proceed?
3. As part of your company's annual performance review process, each employee must identify three coworkers to be interviewed by his manager to get a perspective on the employee's overall work performance. Your friend has offered to give you a glowing performance review if you agree to do the same for him. Truth be told, your friend is not a very dependable worker, and his work is often below minimum standards. However, he is a good friend, and you would hate to upset him. What would you do?
4. You are a recent graduate of a well-respected business school, but you are having trouble getting a job. You worked with a professional résumé service to develop a well-written résumé and placed it on several websites; you also sent it directly to contacts at a dozen companies. So far, you have not even had an invitation for an interview. You know that one of your shortcomings is that you have no real job experience to speak of. You are considering beefing up your résumé by exaggerating the extent of the class project you worked on for a few weeks at your brother-in-law's small consulting firm. You could reword the résumé to make it sound as if you were actually employed there and that your responsibilities were greater than they actually were. What would you do?
5. You have just completed a grueling 10-day business trip calling on two dozen accounts in Latin America. There were even business meetings combined with social events late into the night and on the weekends. On the flight back home at the end of this marathon, you are tired and feeling as if you have not seen your family for a month. As you work on completing your expense report, you say to yourself, "The company does not pay me enough for the work that I do." For more than a few moments, you think about padding your expense report to make up for all the extra hours and time away from your family. Would it be okay to add "extra expenses" to compensate for the hardship of the trip?

Cases

1. VW Cheats on Emissions Testing

Up until late 2015, Volkswagen AG (VW) was the second largest carmaker in the world, with its 590,000 employees producing nearly 41,000 vehicles per day. At that time, the company's prospects seemed bright, with many of its 12 subsidiaries, such as Audi, Bentley, Bugatti, Ducati, Lamborghini, Volkswagen Passenger Cars, and Volkswagen Commercial Vehicles, performing well.

However, the fortunes of VW changed significantly after a large-scale emissions-test cheating scandal became public in September 2015. VW admitted to installing special software designed to deceive emissions-testing procedures in more than 11 million of its cars, starting as far back as 2005. The software sensed when a car was being tested and then activated equipment that reduced emissions. The software deactivated the equipment during normal driving, resulting in emissions that significantly exceeded legal limits, while also reducing fuel consumption and improving the car's torque and acceleration. The illegal software was installed in VW, Audi, and Porsche models that employed several different diesel engine designs that went through frequent updates over a 10-year period.

VW's admissions led to investigations in Germany, the United States, and other countries, as well as dozens of lawsuits filed by customers, shareholders, and car dealerships. The U.S. Department of Justice sued VW in January 2016 on behalf of the Environmental Protection Agency, and in June, VW agreed to a $14.7 billion settlement. This represents the highest fine to date for violations under the Clean Air Act. Additional civil penalties, a criminal settlement, and further state-level fines have not been determined but could add billions more.

Since news of the emissions scandal broke, the company's stock price has dropped 24 percent, from over $182 per share to under $137 by mid-August 2016. In addition, as a result of diminishing sales and uncertainty over future financial penalties, VW has had to relinquish its goal of surpassing Toyota to become the world's largest automaker by 2018.

Understanding VW's history and culture provides background necessary to understanding how this scandal could have occurred. VW was founded in 1937 by the German Labour Front, a national trade union controlled by the Nazi regime, to produce an affordable "people's car" (eventually known as the VW Beetle) designed by Ferdinand Porsche. However, the breakout of World War II interrupted production of the car, and from 1939 to 1945, VW instead produced vehicles for the German army using laborers from nearby concentration camps.

Following the war, the VW plant was slated to be dismantled because it had been used for military production; however, British officer Major Ivan Hirst convinced his commanders of the great potential of the VW Beetle, and the plant soon began producing cars. In 1949, VW passed back to German control under manager Heinrich Nordoff, and the company became a major component of post-war West German revival.

Over the past two decades, the culture of VW has been primarily shaped by two men: Ferdinand Piëch (grandson of Ferdinand Porsche) who was chief executive from 1993 until 2002 and Martin Winterkorn who was chief executive from 2007 until his resignation in 2015 several days after the emissions testing scandal became public.

According to many employees and industry experts, a success-or-else philosophy has existed at VW at least since the time Piëch became CEO. As an example, early in his tenure, Piëch hosted a group of reporters so they could view a prototype of a new sedan intended to leapfrog all of VW's competitors. When a reporter asked what would happen if the engineering team said that they were unable to deliver the many new features and technical innovations promised by the prototype, Piëch declared, “Then I will tell them they are all fired and I will bring in a new team. And if they tell me they can’t do it, I will fire them, too.”

Piëch turned VW into a global giant by acquiring luxury car brands such as Lamborghini and Bentley and by reviving brands such as Bugatti. One of the technologies he championed was turbocharged direct injection (TDI), which remains VW’s trademark technology for diesel engines. TDI improved fuel efficiency and acceleration and helped make diesel engines more practical for passenger cars. VW company policy required that Piëch retire in 2002 at age 65, but he remained on its supervisory board and was involved in the company’s strategic decisions until his forced resignation in April 2015.

Winterkorn rose through the ranks under Piëch’s leadership, holding significant management positions, including head of quality control, head of research and development, chief executive of the Audi division, and finally, CEO at VW. Winterkorn’s leadership style was similar to Piëch’s; both were known for publicly berating subordinates. Winterkorn would go so far as to bang car parts on tables to emphasize a point. He strongly urged European regulators not to impose excessive emission targets on the automotive industry because he felt that there was a lack of time to develop fuel-efficient technology and that such a regulation would further the economic downturn. Under his leadership, VW bought Porsche in 2012 to further its ambition to become the world’s biggest carmaker.

Many critics have argued that the autocratic leadership style of both Piëch and Winterkorn produced a corporate culture that has been described by some as confident, cutthroat, and narrow-minded. This, in turn, created an environment in which employees were apprehensive about contradicting their superiors and afraid to admit mistakes. Engineers were encouraged to compete for promotion and the approval of a management team who seemed to know only one way to manage: be aggressive at all times.

A central question of this scandal—whether VW’s top management knew of the deception—remains. However, many critics claim that the multibillion dollar emissions cheating scandal shows that at the very least, the VW engineers who created and installed the software did not believe company management expected them to act with integrity. If they had, VW would not have cheated and would not be in this mess.

Critical Thinking Questions

1. VW has blamed a small group of engineers for the misconduct and claims that members of its management board did not know of the decade-long deception. Within many organizations, including VW, a high value is placed on people who can deliver results and get things done. This can create a problem known as “normalization of deviance,” where something bad is done by a member of the group in order to achieve a goal but nobody says anything because everyone is expecting that someone else will instead. As a result, more and more bad behavior is tolerated. Perhaps, the VW engineers felt they had no other option when they realized that they could not deliver the combination of great performance, high gas mileage, and low emissions that had been promised. Some observers believe that normalization of deviance was perpetuated because VW kept hiring the same type of people with the same views—engineering graduates who are promotion-obsessed workaholics who have been taught not to say “no” to management’s goals. Do you accept this explanation for the emission scandal at VW? Why or why not?

2. VW must bring in a new CEO and a key board member as a result of the forced resignation of Piëch and Winterkorn. Identify three specific actions that their replacements must do to begin to change the corporate culture at VW.
3. At the time of this writing, it has been alleged that Robert Bosch GmbH, Europe's largest supplier of auto parts, may have had a role in the VW emissions scandal. Bosch supplied the engine control unit that VW programmed to recognize when its diesel vehicles were undergoing emissions tests. However, Bosch states that it is not responsible for how its components are integrated into vehicles by customers. Do research to learn more about what role Bosch may have had in aiding VW in this deception. Do you believe that Bosch should also be sanctioned and/or fined? Why or why not?

Sources: Jack Ewing and Graham Bowley, "The Engineering of VW's Aggressive Ambition," *New York Times*, December 13, 2015, www.nytimes.com/2015/12/14/business/the-engineering-of-volkswagens-aggressive-ambition.html; David Kravets, "VW Software Emissions Scandal Widens to Include Porsche," *Ars Technica*, November 3, 2015, http://arstechnica.com/tech-policy/2015/11/vw-software-emissions-scandal-widens-to-include-porsche; Guilbert Gates, Jack Ewing, Karl Russell, and Derek Watkins "Explaining VW's Emissions Scandal," *New York Times*, September 12, 2016, www.nytimes.com/interactive/2015/business/international/vw-diesel-emissions-scandal-explained.html; Clifford Atiyeh, "Everything You Need to Know about the VW Diesel-Emissions Scandal," *Car and Driver* (blog), July 26, 2016, http://blog.caranddriver.com/everything-you-need-to-know-about-the-vw-diesel-emissions-scandal; Mark Thompson, "Volkswagen Chairman Ferdinand Piëch Resigns," *CNN*, April 25, 2015, http://money.cnn.com/2015/04/25/news/volkswagen-chairman-resign-ferdinand-piech; Tim Bowler, "Volkswagen: From the Third Reich to Emissions Scandal," *BBC News*, October 2, 2015, www.bbc.com/news/business-34358783; A. Paul Eisenstein, "Could Rogue Software Engineers Be Behind VW Emissions Cheating?," *NBC News*, October 9, 2015; Bloomberg, www.nbcnews.com/business/autos/could-rogue-software-engineers-be-behind-vw-emissions-cheating-n441451; Kartikay Mehrotra and Elisabeth Behrmann, "Volkswagen Diesel Scandal Threatens to Ensnare Bosch," *Bloomberg*, August 19, 2016, www.bloomberg.com/news/articles/2016-08-18/bosch-role-in-vw-diesel-cheating-called-key-by-car-owner-lawyers.

2. Toshiba Accounting Scandal

Toshiba Corporation, a Japanese electronics and engineering conglomerate with headquarters in Tokyo, produces a wide range of products, including personal computers, semiconductors, consumer electronics, household appliances, and nuclear power plant systems. The company also provides an array of services, such as those focused on information technology, communications, and nuclear reactor construction and operation.

In May 2015, Toshiba formed an outside panel to investigate potential accounting irregularities at the company. The formation of such an outside panel is an accepted procedure for companies in Japan, where corporate boards of directors are composed primarily of company executives, with few independent outside directors. An outside panel is typically formed to investigate matters that may involve improprieties by senior managers and executives.

Toshiba's CEO, Hisao Tanaka, resigned in July 2015 when the investigation uncovered that he was aware that Toshiba profits had been overstated by a total of $1.2 billion over a seven-year time period. (Further investigation would determine that the amount of the overstatement was closer to $1.9 billion.) Two former CEOs who held membership on the company's board of directors were also implicated in the investigation and stepped down. Six other members of the board also eventually resigned, and Toshiba announced it would appoint several new and independent directors to its board to strengthen external oversight of its management.

The investigatory panel found that “Toshiba had a corporate culture in which management decisions could not be challenged. … Employees were pressured into inappropriate accounting by postponing low reports or moving certain costs into later years.” Managers at Toshiba set such challenging profit targets that subordinates couldn’t meet them without exaggerating the financial results of individual business units. Furthermore, the head of the investigatory panel stated that the scope of their probe had been limited by company management. The investigation of Toshiba’s U.S. nuclear business, Westinghouse Electric Co., was initially declared off limits. Months after a review of that portion of the business was completed, Toshiba took a $2.5 billion write-down on its Westinghouse business.

Following the scandal, Toshiba was removed from the JPX Nikkei Index 400, the stock index that includes the top Japanese companies based on operating income, return on equity, and market value. The move dealt yet another blow to the company’s reputation—inclusion in the stock index matters because investors, including the world’s largest pension funds, use the stock gauge as a benchmark.

In the first quarter following the revelations of the accounting scandal, Toshiba’s sales fell to their lowest level in years, and the firm lost $102 million for the quarter. The price of Toshiba stock shares dropped precipitously, reaching a 36-year low in early 2016. For the quarter ended July 2016, Toshiba reported a slight drop in revenue but generated its first quarterly profit since the accounting scandal. Cost savings generated by the cutting of bonuses and laying off of employees helped boost profits.

The rise of third-party panels is a part of a larger move in Japan to improve corporate compliance following a number of scandals at companies such as IHI Corporation, Livedoor Company, Mitsubishi, Nikko Cordial Corporation, Olympus Corporation, and others. Under Prime Minister Shinzo Abe, the government, companies, and the stock exchanges have sought to encourage foreign investors with the promise of more corporate transparency.

There are, however, several issues with the use of third-party panels to investigate potential improprieties. For instance, it is the practice in Japan for the members of such a panel to accept the scope of the investigation as defined by the company board of directors. This means that the board can pressure the panel to stay clear of sensitive areas of the business. In addition, members of the panel are not directors of the company and so do not have a fiduciary duty to shareholders. (Company directors do have such a duty, which requires them to work to advance the interests of the company, keep corporate information confidential, not use their position to further their private interests, and inform themselves of all material reasonably available before making business decisions.) Furthermore, the panel members have no power to force managers to handover documents.

Toshiba is a 140-year-old company and one of Japan’s best-known brands. The magnitude of the scandal at the company caused Japan’s Finance Minister, Taro Aso, to comment that the irregularities were “woefully regrettable” and had dealt a blow to the country’s efforts to regain the confidence of global investors. Aso noted that if Japanese companies failed to implement appropriate corporate governance, they could lose the market’s trust.

Critical Thinking Questions

1. Observers have commented that a scandal of this magnitude, occurring over such a long period of time, must involve collaboration among a large number of managers—reaching

from the lowest level to the highest level of an organization. Should investigation of the scandal at Toshiba continue until all involved parties are outed and punished? What are the pros and cons of such an action?

2. Do you think that the practice of appointing outside panels to perform investigations should continue, or can you develop a better solution to enforce corporate compliance with laws and generally accepted accounting principles?
3. Japan is generally considered to be struggling in areas such as transparency and board independence compared to the global standard. What measures do you think should be considered at the national level to improve transparency and gain the trust of foreign investors?

Sources: Michael Addady, "Toshiba's Accounting Scandal Is Much Worse than We Thought," *Fortune*, September 8, 2015, http://fortune.com/2015/09/08/toshiba-accounting-scandal; Eric Pfanner and Megumi Fujikawi, "Toshiba Slashes Earnings for Past Seven Years," *Wall Street Journal*, September 7, 2015, www.wsj.com/articles/toshiba-slashes-earnings-for-past-7-years-1441589473; "Toshiba," *New World Encyclopedia,* www.newworldencyclopedia.org/entry/Toshiba (accessed September 20, 2016); Takashi Mochizuki, "Toshiba Posts Profit–WSJ," *Wall Street Journal*, August 13, 2016, http://www.morningstar.com/news/djnmndjbn,paeq/TDJNDN_ 20160813173/toshiba-posts-profit-wsj.html; Megumi Fujikawa, "Japan Chides Canon Over Toshiba Deal," *Wall Street Journal*, July 1, 2016; Yuka Koshino, "Outside Probes Expose Limits of Japan's Corporate Transparency," *Wall Street Journal*, July 22, 2016, www.wsj.com/articles/outsider-probes-expose-limits-of-japans-corporate-transparency-1469171152; Sean Farrell, "Toshiba Boss Quits over £780m Accounting Scandal," *Guardian*, July 21, 2015, www.theguardian.com/world/2015/jul/21/toshiba-boss-quits-hisao-tanaka-accounting-scandal.

End Notes

[1] Alex Wilhelm, "FCC Slams AT&T with $105M Settlement for Bogus Customer Charges," *Tech Crunch*, October 8, 2014, https://techcrunch.com/2014/10/08/fcc-slams-att-with-105m-fine-for-bogus-customer-charges/.

[2] Rebecca R. Ruiz, "F.C.C. to Fine AT&T for Slowing Data Speeds of Some Customers," *New York Times*, June 17, 2015, www.nytimes.com/2015/06/18/technology/fcc-to-fine-att-for-slowing-data-speeds-of-some-customers.html?_r=0.

[3] Todd R. Weiss, "FCC Fines T-Mobile at Least $90M for 'Cramming' Bills," *eWeek*, December 19, 2014, www.eweek.com/mobile/fcc-fines-t-mobile-at-least-90m-for-cramming-bills.html.

[4] Karissa Bell, "FCC Fines Sprint and Verizon $158 Million for Shady Billing Practices," *Mashable*, May 12, 2015, http://mashable.com/2015/05/12/fcc-fines-sprint-verizon/#99zK.gUTGSqa.

[5] Hillary Heuler, "With a Piracy Rate of 80 Percent, Can the Tech World Convince Africa to Buy Legitimate Software?" *ZDNet*, March 31, 2014, www.zdnet.com/article/with-a-piracy-rate-of-80-percent-can-the-tech-world-convince-africa-to-buy-legitimate-software/.

[6] Kim Zetter, "Madoff's Coders Charged with Aiding Massive Ponzi Scheme," *Wired*, November 13, 2009.

[7] Moni Basu, "28 Years for Salmonella: Peanut Exec Gets Groundbreaking Sentence," *CNN*, September 22, 2015, www.cnn.com/2015/09/21/us/salmonella-peanut-exec-sentenced.

[8] Karen Turner, "As Apple's Profits Decline, iPhone Factory Workers Suffer, a New Report Claims," *Washington Post*, September 1, 2016, www.washingtonpost.com/news/the-switch/wp/2016/09/01/as-apples-profits-decline-iphone-factory-workers-suffer-a-new-report-claims.

[9] Zoe Wood, "Tesco's Profits Black Hole Bigger than Expected and Runs Back Several Years," *The Guardian*, October 23, 2014, https://www.theguardian.com/business/2014/oct/23/tesco-profits-black-hole-bigger.

[10] Clifford Atiyeh, "Streak's Over: Fiat Chrysler Admits to Misstating U.S. Sales Reports," *Car and Driver*, July 26, 2016, http://blog.caranddriver.com/streaks-over-fiat-chrysler-admits-to-overstating-u-s-sales-reports/.

[11] "Enron Annual Report 2000," Enron, http://picker.uchicago.edu/Enron/EnronAnnualReport2000.pdf (accessed December 16, 2012).

[12] Gael O'Brien, "The Work Culture at Amazon: Does the Tin Man Have a Heart?" *Business Ethics*, November 13, 2015, http://business-ethics.com/2015/11/13/1252-the-work-culture-at-amazon-does-the-tin-man-have-a-heart/.

[13] Donelson Forsyth, "The Bathsheba Syndrome: When a Leader Fails," *Society for Personality and Social Psychology*, November 13, 2011, http://spsptalks.wordpress.com/2011/11/13/the-bathsheba-syndrome-when-a-leader-fails.

[14] Craig Trudell, "Takata Whistleblower Willing to Testify on Deadly Airbag Flaws," *Automotive News*, February 15, 2015, www.autonews.com/article/20150205/OEM11/150209914/takata-whistleblower-willing-to-testify-on-deadly-airbag-flaws.

[15] "Takata Airbag Recall – Everything You Need to Know," *Consumer Reports*, July 22, 2016, www.consumerreports.org/cro/news/2016/05/everything-you-need-to-know-about-the-takata-air-bag-recall/index.htm.

[16] "National Business Ethics Survey 2013," *Ethics & Compliance Initiative*, www.ethics.org/eci/research/eci-research/nbes/nbes-reports/nbes-2013 (accessed August 11, 2016).

[17] "An Annual Update on Our 2020 Legacy of Good Plan: FY16 Corporate Social Responsibility Report," Dell, Inc., http://i.dell.com/sites/doccontent/corporate/corp-comm/en/Documents/fy15-cr-report.pdf (accessed August 16, 2016).

[18] Dell FY 2016 Corporate Responsibility Report," http://i.dell.com/sites/doccontent/corporate/corp-comm/en/Documents/fy16-cr-report.pdf, accessed August 10, 2016.

[19] John Dudovskiy, "Google Corporate Social Responsibility (CSR)," *Research Methodology*, June 23, 2015, http://research-methodology.net/google-corporate-social-responsibility-csr/.

[20] "2015 Corporate Responsibility Report," IBM, www.ibm.com/ibm/responsibility/2015/assets/downloads/IBM_2015_CR_report.pdf (accessed August 10, 2016).

[21] "Microsoft 2015 Citizenship Report," Microsoft, www.microsoft.com/about/csr/transparencyhub/citizenship-reporting/ (accessed August 10, 2016).

[22] "Oracle Corporate Citizenship Report 2014," Oracle, www.oracle.com/us/corporate/citizenship/corporate-citizenship-report-2563684.pdf (accessed August 10, 2016).

[23] "SAP Integrated Report 2015: Employee and Social Investments," SAP, http://go.sap.com/integrated-reports/2015/en/performance/social/employees-and-social-investments.html (accessed August 10, 2016).

[24] Chad Brooks, “Social Responsibility No Longer Optional for Businesses,” *Business News Daily*, May 22, 2013, www.businessnewsdaily.com/4528-social-responsibility-not-optional.html.

[25] Laura Matthews, “Excedrin Recall 2012 and 5 Other Worse Drug Recalls in FDA History,” *International Business Times*, January 10, 2012, www.ibtimes.com/print/excedrin-recall-2012-and-5-other-worse-drug-recalls-fda-history-393656.

[26] *United States v New York Central & Hudson River R. Co*, 212 U.S. 509 (1909), http://supreme.justia.com/us/212/509/case.html.

[27] Kevin McCoy, “Wells Fargo Fined $185M for Fake Accounts; 5,300 Were Fired,” *USA Today*, September 9, 2016, http://www.usatoday.com/story/money/2016/09/08/wells-fargo-fined-185m-over-unauthorized-accounts/90003212/.

[28] J. Desio Paula, “Ethics and Compliance Programs May Get Their Day in Court,” *Ethics Resource Center*, www.ethics.org/ethics-today/1208/policy-report.html (accessed October 20, 2012).

[29] Suzanne Vranica and Jack Marshall, “Facebook Overestimated Key Video Metric for Two Years,” *Wall Street Journal*, September 22, 2016, http://www.wsj.com/articles/facebook-overestimated-key-video-metric-for-two-years-1474586951.

[30] Arundhati Ramanathan, “IT Firms’ CSR Spending Rose Nearly Five Times in FY15,” *Live Mint*, July 30, 2015, www.livemint.com/Companies/FnLArasuogVLagHMzAFjTK/IT-firms-CSR-spending-rose-nearly-five-times-in-FY15.html.

[31] Ethics Resource Center, “2011 National Business Ethics Survey: Workplace Ethics in Transition,” © 2011, https://s3.amazonaws.com/berkley-center/120101NationalBusinessEthicsSurvey2011WorkplaceEthicsinTransition.pdf.

[32] “National Business Ethics Survey 2013,” *Ethics & Compliance Initiative*, www.ethics.org/eci/research/eci-research/nbes/nbes-reports/nbes-2013 (accessed August 11, 2016).

[33] “What Is an Ethics Officer?” *WiseGEEK*, www.wisegeek.com/what-is-an-ethics-officer.htm (accessed September 20, 2016).

[34] Hannah Clark, “Chief Ethics Officers: Who Needs Them?” *Forbes*, October 23, 2006, www.forbes.com/2006/10/23/leadership-ethics-hp-lead-govern-cx_hc_1023ethics.html.

[35] Hannah Clark, “Chief Ethics Officers: Who Needs Them?” *Forbes*, October 23, 2006, www.forbes.com/2006/10/23/leadership-ethics-hp-lead-govern-cx_hc_1023ethics.html.

[36] Corporate-Ethics US, “Three Main Responsibilities of an Ethics Officer,” www.corporate-ethics.us/EO.htm (accessed October 22, 2012).

[37] Dave Phillips, “Wounded Warrior Board Ousts Top Two Executives,” *CNBC*, March 11, 2016, www.cnbc.com/2016/03/11/wounded-warrior-veterans-nonprofit-fires-ceo-coo-over-big-spending-financial-irregularities.html.

[38] Leo Shane III, “In the Wake of Scandal, Wounded Warrior Project Outlines Significant Overhaul,” *MilitaryTimes*, August 31, 2016, www.militarytimes.com/articles/wwp-overhaul-programs-staff-cuts.

[39] “CR’s 100 Best Corporate Citizens 2016,” *Corporate Responsibility*, www.thecro.com/wp-content/uploads/2016/04/100best_1.pdf (accessed August 9, 2016).

[40] "Dell Supply Chain," Dell, Inc., www.dell.com/learn/us/en/uscorp1/cr-social-responsibility (accessed August 18, 2016).

[41] "National Business Ethics Survey 2013," *Ethics & Compliance Initiative*, www.ethics.org/eci/research/eci-research/nbes/nbes-reports/nbes-2013 (accessed August 11, 2016).

[42] "2015 Corporate Responsibility Report: Governance at IBM," IBM, https://www.ibm.com/ibm/responsibility/2015/governance/governance-at-ibm.html (accessed August 18, 2016).

[43] "National Business Ethics Survey 2013," *Ethics & Compliance Initiative*, www.ethics.org/eci/research/eci-research/nbes/nbes-reports/nbes-2013 (accessed August 11, 2016).

CHAPTER 2

ETHICS FOR IT WORKERS AND IT USERS

QUOTE

Always do right—this will gratify some and astonish the rest.
—Mark Twain

marekuliasz/Shutterstock.com

ORGANIZATIONS BEHAVING BADLY

Queensland, the second largest state in Australia, awarded an outsourcing contract to IBM to build a new payroll application for its Department of Health at an initial cost estimate of $5 million. The project, however, went horribly wrong. Among other issues, the resulting system, delivered many months late, generated incorrect checks for some staff and no checks at all for others. As efforts mounted to fix the problems, the project cost ballooned out of control, eventually reaching more than $1 billion.

Subsequent investigation by the state led to the allegations that IBM employees had acted unethically during the bidding process. In a report issued after the investigation, the Queensland government asserted that it would not have contracted with IBM were it not for misrepresentations made by IBM regarding its expertise as well as the true project costs. For its part, IBM claimed that Queensland employees did a terrible job in managing the project—a claim supported by the state's own investigation.[1,2]

Successful IT outsourcing projects require the development of strong working relationships among members of the client organization and the outside organization that are built on a solid foundation of trust. Unfortunately, many attempts at outsourcing fail—often due to poor working relationships, as this example shows. What are the keys to developing successful working relationships? Who bears responsibility for forming such relationships—the client or the service provider?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What relationships must an IT worker manage, and what key ethical issues can arise in each?
2. What can be done to encourage the professionalism of IT workers?
3. What ethical issues do IT users face, and what can be done to encourage their ethical behavior?

IT WORKER RELATIONSHIPS THAT MUST BE MANAGED

IT workers typically become involved in many different work relationships, including those with employers, clients, suppliers, other professionals, IT users, and society at large. In each relationship, an ethical IT worker acts honestly and appropriately. These various relationships are discussed in the following sections.

Relationships Between IT Workers and Employers

IT workers and employers have a critical, multifaceted relationship that requires ongoing effort by both parties to keep it strong. An IT worker and an employer typically agree on the fundamental aspects of this relationship before the worker accepts an employment offer. These issues may include job title, general performance expectations, specific work responsibilities, drug-testing requirements, dress code, location of employment, salary, work hours, and company benefits. Many other aspects of this relationship may be addressed in a company's policy and procedures manual or in the company's code of conduct, if one exists. Topics addressed in such a manual or code of conduct might include protection of company secrets; vacation policy; time off allowed for a funeral or an illness in the family; tuition reimbursement; and use of company resources, including computers and networks.

Other aspects of this relationship develop over time, depending on circumstances (for example, whether the employee can leave early one day if the time is made up another day). Some aspects are addressed by law—for example, an employee cannot be required to do anything illegal, such as falsify the results of a quality assurance test. Some issues are specific to the role of the IT worker and are established based on the nature of the work or project—for example, the programming language to be used, the type and amount of documentation to be produced, and the extent of testing to be conducted.

As the stewards of an organization's IT resources, IT workers must set an example and enforce policies regarding the ethical use of IT. IT workers often have the skills and knowledge to abuse systems and data or to enable others to do so. Software piracy is an area in which IT workers may be tempted to violate laws and policies. Although end users often get the blame when it comes to using illegal copies of commercial software, software piracy in a corporate setting is sometimes directly traceable to IT staff members—either they allow it to happen or they actively engage in it, often to reduce IT-related spending.

The **Software & Information Industry Association (SIIA)** and the **BSA | The Software Alliance (BSA)** are trade groups that represent the world's largest software and hardware manufacturers. Part of their mission is to stop the unauthorized copying of software produced by its members. North America has the lowest regional rate of software piracy at 17 percent, which represents a commercial value of $10 billion in lost revenue for software development companies.[3] The global software theft rate for personal computer software is around 43 percent, which equates to a commercial value of $62.7 billion.[4]

SIIA promotes the common interests of the software and digital content industry. It protects the intellectual property of member companies and advocates a legal and regulatory environment that benefits the entire industry. SIIA informs the industry and the broader public by serving as a resource on trends, technologies, policies, and related issues that affect member firms and demonstrate the contribution of the industry to the broader economy. It also provides global services in government relations, business development, corporate education, and intellectual property protection. Over 200 organizations are members of SIIA, including 21st Century Fox, Accenture, Adobe Systems, Bank of America Merrill Lynch, Blackboard, Cengage Learning, Fidelity Investments, Google, Scottrade, Thomson Reuters, and Wells Fargo Bank.[5]

BSA is funded both through dues based on member companies' software revenue and through settlements from companies that commit piracy. BSA membership includes about two dozen global members such as Adobe, Apple, Dell, IBM, Intuit, Microsoft, Oracle, and SAS Institute. BSA investigations are usually triggered by calls to the BSA hotline (1-888-NO-PIRACY), reports sent to the BSA website (*www.nopiracy.org*), and referrals from member companies. Many of these cases are reported by disgruntled employees or former employees who can receive a monetary reward of thousands of dollars. In 2012 alone, BSA investigated over 15,000 reports of unlicensed software use around the globe.[6]

When the BSA receives what it believes to be a credible tip, it contacts the company and informs it that a tip has been received. It then requests a detailed inventory of all software used by the company, plus evidence of the appropriate licenses for each piece of software. Should the company have insufficient licenses, it has two choices: purchase the required number of licenses and pay BSA a fine, or stonewall and risk the BSA working with the U.S. Marshall's office to obtain a search warrant to search its premises. Strong probable cause evidence is required to obtain the search warrant, but it has been done in the past resulting in expensive and time-consuming litigation, as well as significant business interruption.

Shortly after its one IT staff member left the company, a Texas automotive repair company received a letter from the BSA accusing it of using unlicensed copies of Microsoft software. The company was threatened with a multimillion-dollar fine, one it could not pay and that would force it out of business. To stave off bankruptcy, the company froze salaries and put off the purchase of needed equipment. The dispute was eventually settled for a fraction of the initial amount after the company sought out legal counsel.[7]

Trade secrecy is another area that can present challenges for IT workers and their employers. A **trade secret** is information, generally unknown to the public, that a company has taken strong measures to keep confidential. It represents something of economic value that has required effort or cost to develop and that has some degree of uniqueness or novelty. Trade secrets can include the design of new software code, hardware designs, business plans, the design of a user interface to a computer program, and manufacturing processes. Examples include the Colonel's secret recipe of 11 herbs and spices used to make the original KFC chicken, the formula for Coke, and Intel's manufacturing process for the Core i7-6950K 10-core processing chip. Employers worry that employees may reveal these secrets to competitors, especially if they leave the company. As a result, companies often require employees to sign confidentiality agreements and promise not to reveal the company's trade secrets.

Zillow is an online real estate and rental marketplace that provides information for people interested in buying, selling, renting, financing, and remodeling homes and apartments. Through the company's website and app, users can access a database of more than 110 million U.S. homes—including homes for sale, homes for rent, and even homes not currently on the market. Zillow also provides a range of services, including one it calls Zestimate, which provides an estimated market value for a house, and a similar service call Rent Zestimate, which estimates the current market rate for rent for a particular property. Move is a rival company offering similar services. In early 2014, Move's chief strategy officer resigned and, on the same day, joined Zillow as its second highest paid executive. Move filed suit against Zillow, alleging that its former employee, and by extension Zillow, stole trade secrets and proprietary information by copying thousands of document and deleting texts and emails from his company-issued computer and smartphone before resigning.[8] Further, Move alleged that Zillow attempted to cover up the theft. Following more than two years of legal wrangling, Zillow agreed to pay Move a total of $130 million to settle the allegations, with the stipulation that Zillow is not admitting liability in the settlement.[9]

Another issue that can create friction between employers and IT workers is whistle-blowing. **Whistle-blowing** is an effort by an employee to attract attention to a negligent, illegal, unethical, abusive, or dangerous act by a company that threatens the public interest. Whistle-blowers often have special information based on their expertise or position within the offending organization. For example, an employee of a computer chip manufacturing company may know that the chemical process used to make the chips is dangerous to employees and the general public. A conscientious employee would call the problem to management's attention and try to correct it by working with appropriate resources within the company. But what if the employee's attempt to correct the problem through internal channels was thwarted or ignored? The employee might then consider becoming a whistle-blower and reporting the problem to people outside the company, including state or federal agencies that have jurisdiction. Obviously, such actions could have negative consequences on the employee's job, perhaps resulting in retaliation and firing.

Amazon, IBM, Microsoft, Oracle, and SAP, along with many other companies, are competing in the rapidly growing cloud services arena. Competition is fierce, and the companies all have an incentive to make their cloud services appear financially successful. However, a whistle-blower lawsuit recently filed against Oracle highlighted potential issues related to the way such companies account for income from subscription-based software services that run in the cloud. The whistle-blower, a former Oracle employee, accused management of pressuring her to add millions of dollars in accruals to financial reports for expected cloud-based software and services revenue. Accounting experts acknowledge that classifying software sales as cloud or traditional is complex and requires determinations that might subsequently be challenged by auditors. Nonetheless, Oracle shares dropped 4 percent the day following announcement of the lawsuit.[10] Although Oracle alleges the whistle-blower was fired for poor performance, the employee maintains that she was let go just two months after she received a positive job performance review and just one month after the alleged incident began. Oracle strongly denies any allegations of wrongdoing and has vowed to countersue the whistle-blower for malicious prosecution.[11]

Relationships Between IT Workers and Clients

IT workers provide services to clients; sometimes those "clients" are coworkers who are part of the same company as the IT worker. In other cases, the client is part of a different company. In relationships between IT workers and clients, each party agrees to provide something of value to the other. Generally speaking, the IT worker provides hardware, software, or services at a certain cost and within a given time frame. For example, an IT worker might agree to implement a new accounts payable software package that meets a client's requirements. The client provides compensation, access to key contacts, and perhaps a work space. This relationship is usually documented in contractual terms—who does what, when the work begins, how long it will take, how much the client pays, and so on. Although there is often a vast disparity in technical expertise between IT workers and their clients, the two parties must work together to be successful.

Typically, the client makes decisions about a project on the basis of information, alternatives, and recommendations provided by the IT worker. The client trusts the IT worker to use his or her expertise and to act in the client's best interests. The IT worker must trust that the client will provide relevant information, listen to and understand what the IT worker says, ask questions to understand the impact of key decisions, and use the information to make wise choices among various alternatives. Thus, the responsibility for decision making is shared between the client and the IT worker.

One potential ethical problem that can interfere with the relationship between IT workers and their clients involves IT consultants or auditors who recommend their own products and services or those of an affiliated vendor to remedy a problem they have detected. Such a situation has the potential to undermine the objectivity of an IT worker due to a **conflict of interest**—a conflict between the IT worker's (or the IT firm's) self-interest and the client's interests. For example, an IT consulting firm might be hired to assess a firm's IT strategic plan. After a few weeks of analysis, the consulting firm might provide a poor rating for the existing strategy and insist that its proprietary products and services are required to develop a new strategic plan. Such findings would raise questions about the vendor's objectivity and the trustworthiness of its recommendations.

Problems can also arise during a project if IT workers find themselves unable to provide full and accurate reporting of the project's status due to a lack of information, tools, or experience needed to perform an accurate assessment. The project manager may want to keep resources flowing into the project and hope that problems can be corrected before anyone notices. The project manager may also be reluctant to share status information because of contractual penalties for failure to meet the schedule or to develop certain system functions. In such a situation, the client may not be informed about a problem until it has become a crisis. After the truth comes out, finger-pointing and heated discussions about cost overruns, missed schedules, and technical incompetence can lead to charges of fraud, misrepresentation, and breach of contract described next.

Fraud is the crime of obtaining goods, services, or property through deception or trickery. Fraudulent misrepresentation occurs when a person consciously decides to induce another person to rely and act on a misrepresentation. To prove fraud in a court of law, prosecutors must demonstrate the following elements:

- The wrongdoer made a false representation of material fact.
- The wrongdoer intended to deceive the innocent party.
- The innocent party justifiably relied on the misrepresentation.
- The innocent party was injured.

Misrepresentation is the misstatement or incomplete statement of a material fact. If the misrepresentation causes the other party to enter into a contract, that party may have the legal right to cancel the contract or seek reimbursement for damages.

Affinity Gaming, a Las Vegas-based casino with 11 properties located across four states, suffered a data breach in 2013 that enabled hackers to gain access to customers' credit card data. Affinity hired Trustwave, an information security company that provides on-demand threat, vulnerability, and compliance-management services to investigate and contain the breach. Following its investigation, Trustwave claimed that it had identified how the data breach had occurred and had contained the malware responsible for it. However, a year later, Affinity was hit with a second customer data breach. This time, Affinity hired Mandiant, a Trustwave competitor, to conduct an investigation. Mandiant concluded that Trustwave's original work was incomplete and had failed to identify the means by which the attacker had breached Affinity's data security. Affinity sued Trustwave for conducting an allegedly "woefully inadequate" investigation that missed key details of the network breach and enabled subsequent attacks. Affinity alleged that Trustwave made misrepresentations when it claimed that its examination would analyze and help remedy the data breach, when it represented that the data breach was "contained," and when it claimed that its recommendations would address the data breach.[12]

Breach of contract occurs when one party fails to meet the terms of a contract. Further, a **material breach of contract** occurs when a party fails to perform certain express or implied obligations, which impairs or destroys the essence of the contract. Because there is no clear line between a minor breach and a material breach, determination is made on a case-by-case basis. "When there has been a material breach of contract, the non-breaching party can either: (1) rescind the contract, seek restitution of any compensation paid under the contract to the breaching party, and be discharged from any further performance under the contract; or (2) treat the contract as being in effect and sue the breaching party to recover damages."[13]

In 2016, Hewlett-Packard Enterprise (HPE) was awarded $3 billion in damages from Oracle after a court determined that Oracle had breached its contract with HPE by dropping support for all Oracle database software being run on HP systems using Intel's Itanium processor chip. HPE argued that Oracle's actions dramatically reduced the sale of HPE's Itanium-based products. HPE also alleged that Oracle's actions were intended to boost sales of Oracle's own Sun hardware. The jury ultimately agreed with HPE and awarded it the full amount it was seeking, compensating the company for both lost sales and damages, as well as requiring Oracle to continue supporting Itanium-based systems.[14]

When IT projects go wrong because of cost overruns, schedule slippage, lack of system functionality, and so on, aggrieved parties might charge fraud, fraudulent misrepresentation, and/or breach of contract. Trials can take years to settle, generate substantial legal fees, and create bad publicity for both parties. As a result, the vast majority of such disputes are settled out of court, and the proceedings and outcomes are concealed from the public. In addition, IT vendors have become more careful about protecting themselves from major legal losses by requiring that contracts place a limit on potential damages.

Most IT projects are joint efforts in which vendors and customers work together to develop a system. Assigning fault when such projects go wrong can be difficult; one side might be partially at fault, while the other side is mostly at fault. Clients and vendors often disagree about who is to blame in such circumstances. Frequent causes of problems in IT projects include the following (see Figure 2-1):

- Scope creep—Changes to the scope of the project or the system requirements can result in cost overruns, missed deadlines, and a project that fails to meet end-user expectations.
- Poor communication—Miscommunication or a lack of communication between customer and vendor can lead to a system whose performance does not meet expectations.
- Delivery of an obsolete solution—The vendor delivers a system that meets customer requirements, but a competitor comes out with a system that offers more advanced and useful features.
- Legacy systems—If a customer fails to reveal information about legacy systems or databases that must connect with the new hardware or software at the start of a project, implementation can become extremely difficult.

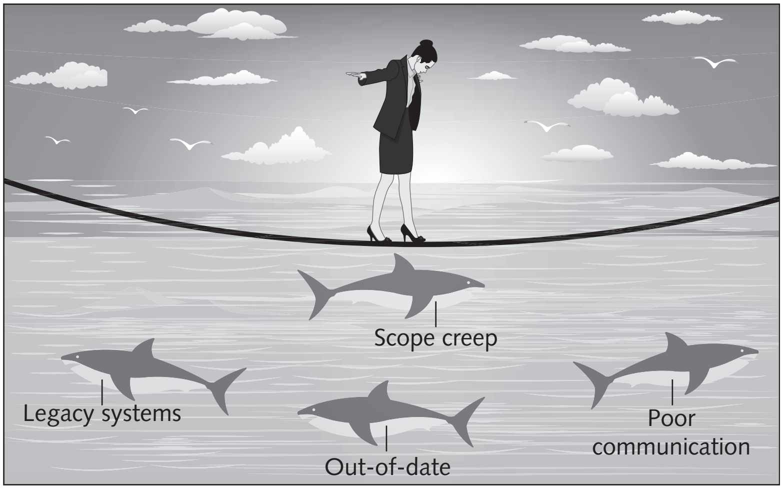


FIGURE 2-1 Frequent causes of problems in IT projects

Relationships Between IT Workers and Suppliers

IT workers deal with many different hardware, software, and service providers. Most IT workers understand that building a good working relationship with suppliers encourages the flow of useful communication as well as the sharing of ideas. Such information can lead to innovative and cost-effective ways of using the supplier's products and services that the IT worker may never have considered.

IT workers can develop good relationships with suppliers by dealing fairly with them and not making unreasonable demands. Threatening to replace a supplier who can't deliver needed equipment tomorrow, when the normal industry lead time is one week, is aggressive behavior that does not help build a good working relationship.

Suppliers strive to maintain positive relationships with their customers in order to make and increase sales. To achieve this goal, they may sometimes engage in unethical actions—for example, offering an IT worker a gift that is actually intended as a bribe. Clearly, IT workers should not accept a bribe from a vendor, and they must be careful when considering what constitutes a bribe. For example, accepting invitations to expensive dinners or payment of entry fees for a golf tournament may seem innocent to the recipient, but it may be perceived as bribery by an auditor.

Bribery is the act of providing money, property, or favors to someone in business or government in order to obtain a business advantage. An obvious example is a software supplier sales representative who offers money to another company's employee to get its business. This type of bribe is often referred to as a kickback or a payoff. The person who offers a bribe commits a crime when the offer is made, and the recipient is guilty of a crime if he or she accepts the bribe. Various states have enacted bribery laws, which have sometimes been used to invalidate contracts involving bribes but have seldom been used to make criminal convictions.

Foxconn Technology, the world's largest electronics contract manufacturer, is headquartered in New Taipei City, Taiwan. The company assembles products for top international brands such as Apple, Nokia, and Sony, and it procures supplies for those products from a wide range of suppliers. In 2014, five former Foxconn employees, including two former senior managers, were charged with bribery for accepting kickbacks from 10 suppliers in exchange for purchasing contracts and assistance clearing Foxconn's quality control checks. Foxconn officials detected the problem and alerted authorities in both Taiwan and China following an internal audit.[15]

Internal control is the process established by an organization's board of directors, managers, and IT systems people to provide reasonable assurance for the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations. An organization's internal control resources include all the people, policies, processes, procedures, and systems controlled by management that enable it to meet these goals (see Figure 2-2).

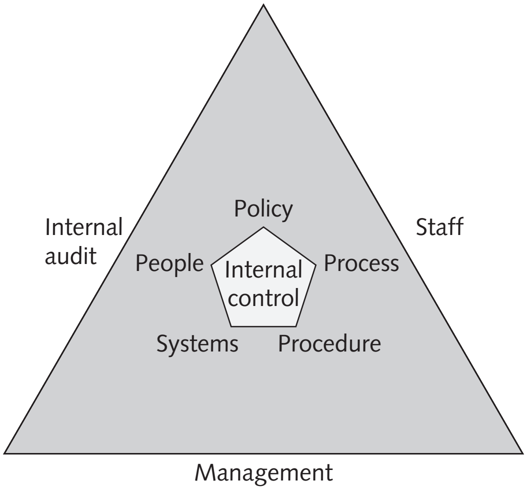


FIGURE 2-2 Internal control

Policies are the guidelines and standards by which the organization must abide. The guidelines and standards are often in response to some law. Policies drive processes and procedures. **Processes** are a collection of tasks designed to accomplish a stated objective. A **procedure** defines the exact instructions for completing each task in a process. An organization might have a policy that defines the credit terms and collection guidelines to be followed when handling a customer order. The processes associated with handling customer orders could include creating a new customer account, accepting a new order from an existing customer, and planning shipment of a customer order, among others. Procedures for each process define how to complete each task in the process. The process and procedures must be designed and executed to conform to the credit terms and collection guidelines policy.

Management is responsible for ensuring that an adequate system of internal control is set up, documented with written procedures, and implemented. Management must also decide the proper level of control over various aspects of the business so that the cost of implementing control does not outweigh the benefits. Employees are responsible for following the documented procedures and reporting to management if the controls are not effective in meeting the needs of the organization. The internal audit organization is responsible for assessing whether the internal controls have been implemented correctly and are functioning as designed; the internal audit organization reports its findings to management.

A fundamental concept of good internal controls is the careful **separation of duties** associated with any process that involves the handling of financial transactions so that different aspects of the process are handled by different people. With proper separation of duties, fraud would require the collusion of two or more parties. When designing an accounts receivable system, for instance, the principal of separation of duties dictates that you separate responsibility for the receipt of customer payments, approving write-offs, depositing cash, and reconciling bank statements. Ideally, no one person should be allowed to perform more than one of these tasks. Internal controls play a key role in preventing and detecting fraud and protecting the organization's resources. Proper separation of duties is frequently reviewed during the audit of a business operation.

In small organizations, it is common for employees to have multiple responsibilities. Separation of duties is often not practical, and internal controls are more likely to be informal and carried out by one or a few people. Such a lack of separation of duties raises concerns that fraud could go undetected. Monitoring and reviewing cash receipt and disbursement activities by supervisory personnel not directly involved with the daily processing is one way to improve internal control within a small organization.

The **Foreign Corrupt Practices Act (FCPA,** 15 U.S. Code § 78dd-1) makes it a crime to bribe a foreign official, a foreign political party official, or a candidate for foreign political office. The act applies to any U.S. citizen or company and to any company with shares listed on any U.S. stock exchange. However, a bribe is not a crime if the payment was lawful under the laws of the foreign country in which it was paid. Penalties for violating the FCPA are severe—corporations face a fine of up to $2 million per violation, and individual violators may be fined up to $100,000 and imprisoned for up to 5 years.

Importantly, the FCPA also requires corporations whose securities are listed in the United States to meet U.S. accounting standards by having an adequate system of internal control, including maintaining books and records that accurately and fairly reflect all transactions—the so-called books and records provision of the act. The goal of these standards is to prevent companies from using slush funds or other means to disguise payments to foreign officials. A firm's business practices and its accounting information systems must be audited by both internal and outside auditors to ensure that they meet these standards. Thus, it is not enough for an organization to simply direct its employees or agents to not accept or offer bribes; rather, it must also keep a set of books and establish a system of internal control to prevent bribery from occurring.

Hewlett-Packard (HP) agreed to pay $108 million to resolve FCPA-related investigations by the U.S. Department of Justice and the Securities and Exchange Commission into whether HP subsidiaries in Mexico, Poland, and Russia bribed government officials to obtain highly profitable contracts. The investigation revealed that HP's "subsidiaries created a slush fund for bribe payments, employed two sets of books to track bribe recipients, and used anonymous email accounts and prepaid mobile telephones to arrange covert meetings to hand over bags of cash," according to Deputy Assistant Attorney General Bruce Swartz. In a statement issued when the settlement was announced, HP executive vice president and general counsel John Schultz said HP fully cooperated with the investigation and that the misconduct was limited to a small number of people who were no longer employed by the company.[16]

In some countries, gifts are an essential part of doing business. In fact, in some countries, it would be considered rude not to bring a present to an initial business meeting. In the United States, a gift might take the form of free tickets to a sporting event from a personnel agency that wants to get on your company's list of preferred suppliers. But, at what point does a gift become a bribe, and who decides?

The key distinguishing factor is that no gift should be hidden. A gift may be considered a bribe if it is not declared. As a result, most companies require that all gifts be declared and that everything but token gifts be declined. Some companies have a policy of pooling the gifts received by their employees, auctioning them off, and giving the proceeds to charity.

When it comes to distinguishing between bribes and gifts, the perceptions of the donor and the recipient can differ. The recipient may believe he received a gift that in no way obligates him to the donor, particularly if the gift was not cash. The donor's intentions, however, might be very different. Table 2-1 shows the key distinctions between bribes and gifts.

TABLE 2-1 Distinguishing between bribes and gifts

Bribes	Gifts
Are made in secret, as they are neither legally nor morally acceptable	Are made openly and publicly, as a gesture of friendship or goodwill
Are often made indirectly through a third party	Are made directly from donor to recipient
Encourage an obligation for the recipient to act favorably toward the donor	Come with no expectation of a future favor for the donor

Relationships Between IT Workers and Other Professionals

Professionals often feel a degree of loyalty to the other members of their profession. As a result, they are often quick to help each other obtain new positions but slow to criticize each other in public. Professionals also have an interest in their profession as a whole, because how it is perceived affects how individual members are viewed and treated. (For example, politicians are not generally thought to be very trustworthy, but teachers are.) Hence, professionals owe each other an adherence to the profession's code of conduct. Experienced professionals can also serve as mentors and help develop new members of the profession.

A number of ethical problems can arise among members of the IT profession. One of the most common is **résumé inflation**, which involves lying on a résumé by, for example, claiming competence in an IT skill that is in high demand. Even though an IT worker might benefit in the short term from exaggerating his or her qualifications, such an action can hurt the profession and the individual in the long run. Many employers consider lying on a résumé as grounds for immediate dismissal. For instance, Yahoo hired Scott Thompson, the president of eBay's PayPal electronic payments unit, as its new CEO in January 2012; however, Thompson resigned less than a year later over discrepancies in his academic record summarized on his résumé.[17] Some studies have shown that around 30 percent of all U.S. job applicants exaggerate their accomplishments, while roughly 10 percent "seriously misrepresent" their backgrounds.[18] Table 2-2 lists the areas of a résumé that are most prone to exaggeration.

TABLE 2-2 Most frequent areas of résumé falsehood or exaggeration

Area of exaggeration	Frequency (%)	How to uncover the truth
Embellished skill set	57	Verification of licenses and/or certifications with accrediting agency
Embellished responsibilities	55	Thorough background and reference checks
Dates of employment	42	Thorough background and reference check
Job title	34	Thorough background and reference check
Academic degrees earned	33	Verification of education claims with educational institutions
Companies worked for	26	Thorough background and reference check
Accolades/Awards	18	Thorough background and background check

Source: "Infographic: The Lies We Tell on Resumes," Background Checks.org, http://backgroundchecks.org/infographic-the-lies-we-tell-on-resumes.html.

Another ethical issue that can arise in relationships between IT workers and other professionals is the inappropriate sharing of corporate information. Because of their roles, IT workers may have access to corporate databases of private and confidential information about employees, customers, suppliers, new product plans, promotions, budgets, and so on. It might be sold to other organizations or shared informally during work conversations with others who have no need to know. Revealing such private or confidential information is grounds for termination in many organizations and could even lead to criminal charges.

The Office of Communications (aka Ofcom) is the regulatory and competition authority for the broadcasting, telecommunications, and postal industries in the United Kingdom. In 2016, Ofcom made headlines when one of its former short-term contract employees offered his new employer (UKTV, a multichannel broadcaster jointly owned by BBC Worldwide and Scripps Networks Interactive), six years of confidential income and spending data of competing broadcasters that had been submitted to Ofcom in its regulatory capacity. The data were stolen from Ofcom's market intelligence database and would have provided valuable insights into competitors' programming budgets and revenue streams. UKTV management acted quickly to fire the individual and reported the incident to Ofcom. In a letter to other broadcasters, UKTV promised that it had removed all the data from its systems, assuring its rivals that the data had not been used.[19]

Relationships Between IT Workers and IT Users

The term **IT user** refers to a person who uses a hardware or software product; the term distinguishes end users from the IT workers who develop, install, service, and support the product. IT users need the product to deliver organizational benefits or to increase their productivity.

IT workers have a duty to understand a user's needs and capabilities and to deliver products and services that best meet those needs—subject, of course, to budget and time constraints. They also have a key responsibility to establish an environment that supports ethical behaviors by users. Such an environment discourages software piracy, minimizes the inappropriate use of corporate computing resources, and avoids the inappropriate sharing of information.

Relationships Between IT Workers and Society

Regulatory laws establish safety standards for products and services to protect the public. However, these laws are less than perfect, and they cannot safeguard against all negative side effects of a product or process. Often, professionals can clearly see the effect their work will have and can take action to eliminate potential public risks. Thus, society expects members of a profession to provide significant benefits and to not cause harm through their actions. One approach to meeting this expectation is to establish and maintain professional standards that protect the public.

Clearly, the actions of an IT worker can affect society. For example, a systems analyst may design a computer-based control system to monitor a chemical manufacturing process. A failure or an error in the system may put workers or people who live near the plant at risk. As a result, IT workers have a relationship with members of society who may be affected by their actions. There is currently no single, formal organization of IT workers that takes responsibility for establishing and maintaining standards that protect the public. However, as discussed in the following sections, there are a number of professional organizations that provide useful professional codes of ethics to guide actions that support the ethical behavior of IT workers.

CRITICAL THINKING EXERCISE: ACCEPT THE TICKETS OR NOT?

You are leading your organization's effort to purchase and install new accounting software. The project will cost an estimated $3 million, and over the past few months, you have had meetings with several potential vendors to evaluate their offerings and capabilities. It is early March, and the National Collegiate Athletic Association (NCAA) basketball tournament is underway. You receive a phone call from one of the sales reps you met with recently. He has two tickets to the second-round games next weekend and wants to give them to you. Can you accept this offer without raising any concerns? How can you turn down this offer without offending the sales rep? Would accepting the offer from the sales rep obligate you in any way? Would you feel compelled to share information with him about where his firm stands in the competition for your business? Would you provide him with any insights about how his firm could make its bid more attractive? Would you be more inclined to spend additional time interacting with him to better understand his firm's products and services?

ENCOURAGING THE PROFESSIONALISM OF IT WORKERS

A professional is one who possesses the skill, good judgment, and work habits expected from a person who has the training and experience to do a job well. Organizations—including many IT organizations—are desperately seeking workers who have the following characteristics of a professional:

- They are an expert in the tools and skills needed to do their job.
- They adhere to high ethical and moral standards.
- They produce high quality results.
- They meet their commitments.
- They communicate effectively.
- They train and develop others who are less skilled or experienced.

IT workers of all types can improve their profession's reputation for professionalism by (1) subscribing to a professional code of ethics, (2) joining and participating in professional organizations, (3) obtaining appropriate certifications, and (4) supporting government licensing where available. Each of these topics is discussed in the following sections.

Professional Codes of Ethics

A **professional code of ethics** states the principles and core values that are essential to the work of a particular occupational group. Practitioners in many professions subscribe to a code of ethics that governs their behavior. For example, doctors adhere to varying versions of the 2,000-year-old Hippocratic oath, which medical schools offer as an affirmation to their graduating classes. Most codes of ethics created by professional organizations have two main parts: The first outlines what the organization aspires to become and the second typically lists rules and principles by which members of the organization are expected to abide. Many codes also include a commitment to continuing education for those who practice the profession.

Laws do not provide a complete guide to ethical behavior. Nor can a professional code of ethics be expected to provide an answer to every ethical dilemma—no code can be a definitive collection of behavioral standards. However, following a professional code of ethics can produce many benefits for the individual, the profession, and society as a whole:

- *Ethical decision making*—Adherence to a professional code of ethics means that practitioners use a common set of core values and beliefs as a guideline for ethical decision making.
- *High standards of practice and ethical behavior*—Adherence to a code of ethics reminds professionals of the responsibilities and duties that they may be tempted to compromise to meet the pressures of day-to-day business. The code also defines acceptable and unacceptable behaviors to guide professionals in their interactions with others. Strong codes of ethics have procedures for censuring professionals for serious violations, with penalties that can include the loss of the right to practice. Such codes are the exception, however, and few exist in the IT arena.
- *Trust and respect from the general public*—Public trust is built on the expectation that a professional will behave ethically. People must often depend on the integrity and good judgment of a professional to tell the truth, abstain from giving self-serving advice, and offer warnings about the potential negative side effects of their actions. Thus, adherence to a code of ethics enhances trust and respect for professionals and their profession.
- *Evaluation benchmark*—A code of ethics provides an evaluation benchmark that a professional can use as a means of self-assessment. Peers of the professional can also use the code for recognition or censure.

Professional Organizations

No one IT professional organization has emerged as preeminent, so there is no universal code of ethics for IT workers. However, the existence of such organizations is useful in a field that is rapidly growing and changing. In order to stay on the top of the many new developments in their field, IT workers need to network with others, seek out new ideas, and continually build on their personal skills and expertise. Whether you are a freelance programmer or the CIO of a *Fortune* 500 company, membership in an organization of IT workers enables you to associate with others of similar work experience, develop working relationships, and exchange ideas. These organizations disseminate information through email, periodicals, websites, social media, meetings, and conferences. Furthermore, in recognition of the need for professional standards of competency and conduct, many of these organizations have developed codes of ethics. Four of the most prominent IT-related professional organizations are highlighted in the following sections.

Association for Computing Machinery (ACM)

The Association for Computing Machinery (ACM), a computing society founded in New York in 1947, is "dedicated to advancing the art, science, engineering, and application of information technology, serving both professional and public interests by fostering the open interchange of information and by promoting the highest professional and ethical standards."[20] ACM is the world's largest educational and scientific society and is international in scope, with ACM councils established in Europe, India, and China. Over half the organization's 100,000 student and professional members reside outside the United States in more than 100 countries. Its leading magazine, *Communications of the ACM*, provides industry news, commentary, observations, and practical research. In addition, the ACM sponsors 37 special-interest groups (SIGs) representing major areas of computing. Each group provides publications, workshops, and conferences for information exchange.[21] The ACM Code of Ethics can be found at *https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct#top*.

Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS)

The Institute of Electrical and Electronics Engineers (IEEE) covers the broad fields of electrical, electronic, and information technologies and sciences. The IEEE-CS is one of the oldest and largest IT professional associations, with about 60,000 members. Founded in 1946, the IEEE-CS is the largest of the 38 societies of the IEEE. The society sponsors many conferences, applications-related and research-oriented journals, local and student chapters, technical committees, and standards working groups.[22]

Association of Information Technology Professionals (AITP)

The Association of Information Technology Professionals (AITP) started in Chicago in 1951, when a group of machine accountants got together and decided that the future was bright for the IBM punched-card tabulating machines they were operating—a precursor of the modern electronic computer. They were members of a local group called the Machine Accountants Association (MAA), which first evolved into the Data Processing Management Association in 1962 and finally the AITP in 1996.[23]

The AITP provides IT-related seminars and conferences, information on IT issues, and forums for networking with other IT workers. Its mission is to provide superior leadership and education in information technology, and one of its goals is to help members make themselves more marketable within their industry. The AITP also has a code of ethics and standards of conduct. The standards of conduct are considered to be rules that no true IT professional should violate. The AITP Code of Ethics and Standards of Conduct can be found at *https://www.aitp.org/?page=EthicsConduct*.

SysAdmin, Audit, Network, Security (SANS) Institute

The SysAdmin, Audit, Network, Security (SANS) Institute provides information security training and certification for a wide range of individuals, such as auditors, network administrators, and security managers. Each year, its programs train some 12,000 people, and a total of more than 165,000 security professionals around the world have taken one or more of its courses. SANS publishes a semiweekly news digest (*NewsBites*), a weekly security vulnerability digest (*@Risk*), and flash security alerts.[24]

At no cost, SANS makes available a collection of some 1,200 research documents about various information security topics. SANS also operates Internet Storm Center—a program that monitors malicious Internet activity and provides a free early warning service to Internet users—and works with Internet service providers to thwart malicious attackers. The SANS Institute IT Code of Ethics can be found at *https://www.sans.org/security-resources/ethics?ref=3781*.

Certification

Certification indicates that a professional possesses a particular set of skills, knowledge, or abilities, in the opinion of the certifying organization. Unlike licensing, which applies only to people and is required by law, certification can also apply to products (for example, the Wi-Fi CERTIFIED logo assures that the product has met rigorous interoperability testing to ensure that it will work with other Wi-Fi-certified products) and is generally voluntary. IT-related certifications may or may not include a requirement to adhere to a code of ethics, whereas such a requirement is standard with licensing.

Numerous companies and professional organizations offer certifications, and opinions are divided on their value. Many employers view them as a benchmark that indicates mastery of a defined set of basic knowledge. On the other hand, because certification is no substitute for experience and doesn't guarantee that a person will perform well on the job, some hiring managers are rather cynical about the value of certifications. Most IT employees are motivated to learn new skills, and certification provides a structured way of doing so. For such people, completing a certification provides clear recognition and correlates with a plan to help them continue to grow and advance in their careers. Others view certification as just another means for product vendors to generate additional revenue with little merit attached.

Deciding on the best IT certification—and even whether to seek a certification—depends on the individual's career aspirations, existing skill level, and accessibility to training (Table 2-3). Is certification relevant to your current job or the one to which

TABLE 2-3 Common IT industry certifications

Category	Certification	Certifying organization
Security	CompTIA Security+	Computer Technology Industry Association
Security	Certified Security Analyst	International Council of E-commerce Consultants (EC)
Forensics	Certified Computer Examiner	The International Society of Forensic Computer Examiners
Governance	Certified in the Governance of Enterprise IT	ISACA
Project management	Project Management Professional	Project Management Institute

you aspire? Does the company offering the certification have a good reputation? What is the current and potential future demand for skills in this area of certification?

Vendor Certifications

Many IT vendors—such as Cisco, IBM, Microsoft, SAP, and Oracle—offer certification programs for those who use their products. Workers who successfully complete a program can represent themselves as certified users of a manufacturer's product. Depending on the job market and the demand for skilled workers, some certifications might substantially improve an IT worker's salary and career prospects. Certifications that are tied to a vendor's product are relevant for job roles with very specific requirements or certain aspects of broader roles. Sometimes, however, vendor certifications are too narrowly focused on the technical details of the vendor's technology and do not address more general concepts.

To become certified, one must pass a written exam. Because of legal concerns about whether other types of exams can be graded objectively, most exams are presented in a multiple-choice format. A few certifications, such as the Cisco Certified Internetwork Expert (CCIE) certification, also require a hands-on lab exam that demonstrates skills and knowledge. It can take years to obtain the necessary experience required for some certifications. Courses and training material are available to help speed up the preparation process, but such support can be expensive. Depending on the certification, study materials can cost $1,000 or more, and in-class formal training courses often cost more than $10,000. Table 2-4 lists some of the common vendor certifications.

TABLE 2-4 Common vendor-specific certifications for IT workers

Category	Certification
MAC OS X	Apple Certified Technical Coordinator
Cisco Hardware	Cisco Certified Design Associate
Cisco Networking	Cisco Certified Network Professionals
Cisco Networking	Cisco Certified Internetwork Expert
Microsoft Products	Microsoft Certified Professional
Citrix Products	Citrix Certified Administrator (CCA)
Oracle Database	Oracle Database 12c: Certified Expert Performance Management and Tuning
Salesforce software	Salesforce.com Certified Administrator

Licensing of IT Professionals

In the United States, a **government license** is government-issued permission to engage in an activity or to operate a business. Most states license activities that could result in damage to public health, safety, or welfare—if practiced by an individual who has not demonstrated minimal competence. Licensing is generally administered at the state level and often requires that the recipient pass a test of some kind. Some professionals must be licensed, including certified public accountants (CPAs), lawyers, doctors, various types of medical and daycare providers, and some engineers.

The Case for Licensing IT Workers

The days of simple, stand-alone information systems are over. Modern systems are highly complex, interconnected, and critically dependent on one another, and every day, the public entrust their health, safety, and welfare to these systems. Software systems are embedded in the vehicles we drive, controlling functions such as braking, cruise control, airbag deployment, navigation, and parking. Even more advanced systems are being designed and built for "self-driving" vehicles. Complex computers and information systems manage and control the autopilot functions of passenger planes, the nuclear reactors of power plants, and the military's missile launch and guidance systems. Complex medical information systems monitor hospital patients on critical life support. Failure of any of these systems can result in human injury or even death.

As a result of the increasing importance of IT in our everyday lives, the development of reliable, effective information systems has become an area of mounting public concern. This concern has led to a debate about whether the licensing of IT workers would improve information systems. Proponents argue that licensing would strongly encourage IT workers to follow the highest standards of the profession and practice a code of ethics. Without licensing, there are no clear, well-defined requirements for heightened care and no concept of professional malpractice. State licensing boards have ultimate authority over the specific requirements for licensing in their jurisdiction, and also decide whether or not to even offer a given exam.

In 1993, the ACM and IEEE-CS formed a Joint Steering Committee for the Establishment of Software Engineering as a Profession. The initial recommendations of the committee were to define ethical standards, to define the required body of knowledge and recommended practices in software engineering, and to define appropriate curricula to acquire knowledge. The core **body of knowledge** for any profession outlines agreed-upon sets of skills and abilities that all licensed professionals must possess. The "Software Engineering Code of Ethics and Professional Practice" documents the ethical and professional responsibilities and obligations of software engineers. (A **software engineer** is defined as one who applies engineering principles and practices to the design, development, implementation, testing, and maintenance of software.) After a thorough review process, version 5.2 of the Software Engineering Code of Ethics and Professional Practice was adopted by both the ACM and IEEE-CS (see Figure 2-3).[25] The code contains eight principles related to the behavior of and decisions made by software engineers, including practitioners, educators, managers, supervisors, and policy makers, as well as trainees and students of the profession.

The nonprofit organization National Council of Examiners for Engineering and Surveying (NCEES) develops, administers, and scores the examinations used for engineering and surveying licensure in the United States. Members of NCEES include the licensing

Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:

1. Public - Software engineers shall act consistently with the public interest.
2. Client and Employer - Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.
3. Product - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
4. Judgment - Software engineers shall maintain integrity and independence in their professional judgment.
5. Management - Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
6. Profession - Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
7. Colleagues - Software engineers shall be fair to and supportive of their colleagues.
8. Self - Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

FIGURE 2-3 Software Engineering Code of Ethics and Professional Practice

Source: Software Engineering Code of Ethics and Professional Practice. © acm.org, 2015. http://www.acm.org/about/se-code

boards for all 50 states.[26] In 2013, NCEES began offering testing for software engineers. The eight-hour exam consisting of 80 multiple-choice questions was produced in collaboration with the Institute of Electrical and Electronic Engineers (IEEE).[27] As of 2015, 40 states and U.S. jurisdictions support the licensing of software engineers. The software engineering license certifies that the license holder has:

- completed an appropriate engineering education from a program accredited by the Accreditation Board for Engineering and Technology/Engineering Accreditation. (As of October 2015, there are 23 accredited software engineering programs in the United States and 239 computer engineering programs in the United States.)
- at least four years of software engineering experience in his or her field (the required years of experience varies by state) working under the supervision of qualified engineers. (This could be a sticking point because there are so few licensed software engineers.)
- passed the following two NCEES engineering exams: (1) the Fundamentals of Engineering exam, which is a broad-based exam and (2) an eight-hour software engineering Principles and Practices exam, which covers topics such as software requirements, design, construction, testing, maintenance, configuration management, engineering processes, quality assurance, safety, security, and privacy.
- kept current by meeting his or her state's minimum continuing education requirements.

IT Professional Malpractice

For most IT workers, becoming licensed as a software engineer is optional because they practice under the “industrial exemption” clause of their state’s licensing laws that permits them to work internally for an organization without licensure so long as they are not making final decisions to release product to the public or offering engineering services directly to the public (for example, software engineering consultant). However, to open a software engineering consulting practice or to claim that one is a software engineer in a formal context may now require a license in some states. For an IT worker to become licensed raises some potential legal issues, as discussed in the following paragraphs.

Negligence is defined as not doing something that a reasonable person would do or doing something that a reasonable person would not do. **Duty of care** refers to the obligation to protect people against any unreasonable harm or risk. For example, people have a duty to keep their pets from attacking others and to operate their cars safely. Similarly, businesses must keep dangerous pollutants out of the air and water, make safe products, and maintain safe operating conditions.

The courts decide whether parties owe a duty of care by applying a **reasonable person standard** to evaluate how an objective, careful, and conscientious person would have acted in the same circumstances. Likewise, defendants who have particular expertise or competence are measured against a **reasonable professional standard**. For example, in a medical malpractice suit based on improper treatment of a broken bone, the standard of measure would be higher if the defendant were an orthopedic surgeon rather than a general practitioner. In the IT arena, consider a hypothetical negligence case in which an employee inadvertently destroyed millions of customer records in an Oracle database. The standard of measure would be higher if the defendant were a licensed software engineer certified as an Oracle database administrator (DBA) with 10 years of experience rather than an unlicensed systems analyst with no DBA experience or specific knowledge of the Oracle software.

If a court finds that a defendant actually owed a duty of care, it must then determine whether the duty was breached. A **breach of the duty of care** is the failure to act as a reasonable person would act. A breach of duty might consist of an action, such as throwing a lit cigarette into a fireworks factory and causing an explosion, or a failure to act when there is a duty to do so—for example, a police officer not protecting a citizen from an attacker.

Professionals who breach the duty of care are liable for injuries that their negligence causes. This liability is commonly referred to as **professional malpractice**. For example, a CPA who fails to use reasonable care, knowledge, skill, and judgment when auditing a client’s books is liable for accounting malpractice. Professionals who breach this duty are liable to their patients or clients and possibly to some third parties.

In the past, courts have consistently rejected attempts to sue individual parties for computer-related malpractice (see *Chatlos Systems, Inc., Plaintiff v. National Cash Register Corporation, Defendant* 479 F.Supp. 738 (1979)). Professional negligence can occur only when people fail to perform within the standards of their profession, and software engineering, until recently, was not a licensed profession in the United States. Because there were no uniform standards against which to compare a software engineer’s professional behavior, he or she could not be subject to malpractice lawsuits.

CRITICAL THINKING EXERCISE: RAISING THE LEVEL OF PROFESSIONALISM AT AN IT CONSULTING FIRM

You are a member of the human resources group of an IT consulting firm with some three dozen consultants. You are considering initiating a program to encourage more of the consultants to join IT-professional organizations and to earn more IT-related certifications. Identify three business benefits of doing this. What incentives might you offer to the consultants to encourage them to join professional organizations and gain more certifications? What resistance might you expect from some of the staff? How might you overcome this resistance?

WHAT CAN BE DONE TO ENCOURAGE THE ETHICAL USE OF IT RESOURCES AMONG USERS?

This section discusses some of the most common ethical issues that IT users face, as well as ways that organizations can encourage the ethical use of IT by their employees, an area of growing concern as more companies provide employees with smartphones, tablets, and laptops—along with PCs, and other devices—to access corporate information systems, data, and the Internet.

Common Ethical Issues for IT Users

This section discusses a few common ethical issues faced by IT users. Additional ethical issues will be discussed in future chapters.

Software Piracy

As mentioned earlier in this chapter, software piracy in a corporate setting can sometimes be directly traceable to IT professionals—they might allow it to happen, or they might actively engage in it. Corporate IT usage policies and management should encourage users to report instances of piracy and to challenge its practice. The software piracy rates in Albania, Kazakhstan, Libya, Panama, and Zimbabwe exceed 70 percent, so it is clear that business managers and IT professionals in those countries do not take a strong stand against the practice.[28]

Sometimes IT users are the ones who commit software piracy. A common violation occurs when employees copy software from their work computers for use at home. When confronted, the IT user's argument might be: "I bought a home computer partly so I could take work home and be more productive; therefore, I need the same software on my home computer as I have at work." However, if no one has paid for an additional license to use the software on the home computer, this is still piracy.

The increasing popularity of the Android smartphone operating system has created a serious software piracy problem. Some IT end users have figured out how to download applications from the Google Play store without paying for them, and then use the software or sell it to others. Indeed, the rate of software piracy for apps from Google's Play store is alarmingly high—exceeding 90 percent for some popular games such as Monument Valley. The software piracy rate for that same game from Apple's App store is closer to 60 percent.[29] Software piracy can have a negative impact on future software development if professional developers become discouraged watching revenue from legitimate sales sink while the sales of pirated software and games skyrocket.

Inappropriate Use of Computing Resources

Some employees use their computers to surf popular websites that have nothing to do with their jobs, participate in chat rooms, view pornographic sites, and play computer games. These activities eat away at a worker's productivity and waste time. Furthermore, activities such as viewing sexually explicit material, sharing lewd jokes, and sending hate email could lead to lawsuits and allegations that a company allowed a work environment conducive to racial or sexual harassment. A survey by the Fawcett Society found that one in five men admit to viewing porn at work, while a separate study found that 30 percent of mobile workers are viewing porn on their web-enabled phones.[30,31] Organizations typically fire frequent pornography offenders and take disciplinary action against less egregious offenders.

Inappropriate Sharing of Information

Every organization stores vast amounts of information that can be classified as either private or confidential. Private data describe individual employees—for example, their salary information, attendance data, health records, and performance ratings. Private data also include information about customers—credit card information, telephone number, home address, and so on. Confidential information describes a company and its operations, including sales and promotion plans, staffing projections, manufacturing processes, product formulas, tactical and strategic plans, and research and development. An IT user who shares this information with an unauthorized party, even inadvertently, has violated someone's privacy or created the potential that company information could fall into the hands of competitors. For example, if an employee accessed a coworker's payroll records via a human resources computer system and then discussed them with a friend, it would be a clear violation of the coworker's privacy.

One of the most serious leaks of sensitive information in the U.S. history occurred in late 2010, when hundreds of thousands of leaked State Department documents were posted on the WikiLeaks' website. The source of the leaks was a low-level IT user (an army private) with access to confidential documents. The documents revealed details of behind-the-scene international diplomacy, often divulging candid comments from world leaders and providing particulars of U.S. tactics in Afghanistan, Iran, and North Korea.[32] The leaked documents strained relations between the United States and some of its allies. It is also possible that the incident will cause other countries to be less willing to share sensitive information with the United States because of concerns over further disclosures.

There have been many other instances of the breach of sensitive information by an organization's IT users. For example, a Morgan Stanley financial adviser was fired after the firm accused him of stealing the account data of almost 350,000 clients and posting some of that information for sale online. The former employee was also convicted of criminal charges, sentenced to probation, and ordered to pay restitution. In addition, Morgan Stanley paid a $1 million fine to the Securities and Exchange Commission (SEC) for its failure to protect its customers' data.[33,34]

Supporting the Ethical Practices of IT Users

The growing use of IT has increased the potential for new ethical issues and problems; thus, many organizations have recognized the need to develop policies that protect against abuses. Although no policy can stop wrongdoers, it can set forth the general rights and responsibilities of all IT users, establish boundaries of acceptable and unacceptable behavior, and enable management to punish violators. Adherence to a policy can improve services to users, increase productivity, and reduce costs. Companies can take several actions when creating an IT usage policy, as discussed in the following sections.

Establishing Guidelines for Use of Company Hardware and Software

Company IT managers must provide clear rules that govern the use of home computers and associated software. Some companies negotiate contracts with software manufacturers and provide PCs and software so that IT users can work at home. Other companies help employees buy hardware and software at corporate discount rates. The goal should be to ensure that employees have legal copies of all the software they need to be effective, regardless of whether they work in an office, on the road, or at home.

Defining an Acceptable Use Policy

An **acceptable use policy (AUP)** is a document that stipulates restrictions and practices that a user must agree to in order to use organizational computing and network resources. It is an essential information security policy—so important that most organizations require that employees sign an acceptable use policy before being granted a user or network ID. An effective acceptable use policy is clear and concise and contains the following five key elements:

1. Purpose of the AUP—Why is the policy needed and what are its goals?
2. Scope—Who and what is covered under the AUP?
3. Policy—How are both acceptable use and unacceptable use defined; what are some examples of each?
4. Compliance—Who is responsible for monitoring compliance and how will compliance will be measured?
5. Sanctions—What actions will be taken against an individual who violates the policy?

Members of the legal, human resources, and information security groups are involved in creating the AUP. It is the organization's information security group that is responsible for monitoring compliance to the AUP. **Information security (infosec) group's** responsibilities include managing the processes, tools, and policies necessary to prevent, detect, document, and counter threats to digital and nondigital information, whether it is in transit, being processed, or at rest in storage.

Table 2-5 provides a manager's checklist for establishing an effective acceptable use policy. The preferred answer to each question is *yes*.

For a sample of an acceptable use policy created by SANS Institute, the largest provider of cybersecurity training and certification to professionals at governments and commercial institutions worldwide, visit *https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy*.

TABLE 2-5 Manager's checklist for establishing an acceptable use policy

Question	Yes	No
Is there a statement that explains the need for an acceptable use policy?		
Is it clear how the policy applies to the following types of workers? • Full-time employees • Part-time employees • Temps • Contractors		
Does the policy address the following issues? • Protection of the data privacy rights of employees, customers, suppliers, and others • Control of access to proprietary company data and information • Use of unauthorized or pirated software • Employee monitoring, including email, wiretapping and eavesdropping on phone conversations, computer monitoring, and surveillance by video • Respect of the intellectual rights of others, including trade secrets, copyrights, patents, and trademarks • Inappropriate use of IT resources, such as web surfing, excessive use of social networks, blogging, personal emailing, and other use of computers for purposes other than business • The need to protect the security of IT resources through adherence to good security practices, such as not sharing user IDs and passwords, using hard-to-guess passwords, and frequently changing passwords • The use of the computer to intimidate, harass, or insult others through abusive language in emails and by other means		
Are disciplinary actions defined for IT-related abuses?		
Is there a process for communicating the policy to employees?		
Is there a plan to provide effective, ongoing training relative to the policy?		

Structuring Information Systems to Protect Data and Information

Organizations must implement systems and procedures that limit data access to just those employees who need it. For example, sales managers may have total access to sales and promotion databases through a company network, but their access should be limited to products for which they are responsible. Furthermore, they should be prohibited from accessing data about research and development results, product formulas, and staffing projections if they don't need it to do their jobs.

Installing and Maintaining a Corporate Firewall

A **firewall** is hardware or software (or a combination of both) that serves as the first line of defense between an organization's network and the Internet; a firewall also limits access to the company's network based on the organization's Internet-usage policy. A firewall can be configured to serve as an effective deterrent to unauthorized web surfing by blocking access to specific objectionable websites. (Unfortunately, the number of such sites is continually growing, so it is difficult to block them all.) A firewall can also serve as an effective barrier to incoming email from certain websites, companies, or users. It can even be programmed to block email with certain kinds of attachments (for example, Microsoft Word documents), which reduces the risk of harmful computer viruses.

Compliance

Compliance means to be in accordance with established policies, guidelines, specifications, or legislation. Records management software, for example, may be developed in compliance with the U.S. Department of Defense's Design Criteria Standard for Electronic Management Software applications (known as DoD 5015) that defines mandatory functional requirements for records management software used within the Department of Defense. Commercial software used within an organization should be distributed in compliance with the vendor's licensing agreement.

In the legal system, compliance usually refers to behavior in accordance with legislation—such as the Sarbanes–Oxley Act of 2002, which established requirements for a system of internal control to govern the creation and documentation of accurate and complete financial statements, or the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), which requires employers to ensure the security and privacy of employee healthcare data. Failure to be in compliance with specific pieces of legislation can lead to criminal or civil penalties specified in that legislation.

Failure to be in compliance with legislation can also lead to lawsuits or government fines. For instance, the California Online Privacy Protection Act of 2003 requires "commercial operators of online services, including mobile and social apps, which collect personally identifiable information from Californians, to conspicuously post a privacy policy," according to the California Attorney General's office. Such a policy must outline what data are gathered, for what purposes the data are being collected, and with whom the data may be shared. Developers of mobile applications face fines of up to $2,500 for every noncompliant application that is downloaded. Several organizations, including Delta, United Airlines, and Open Table, were notified by the Attorney General's office in late 2012 that they were not in compliance and were given 30 days to provide specific plans and a timeline for becoming compliant with the law.[35]

It is a major challenge for many organizations to maintain compliance with multiple government and industry regulations, which are frequently updated and modified so that regulations have similar but sometimes conflicting requirements. For example, the California Online Privacy Protection Act of 2003 was amended in 2013 by Assembly Bill 370, which requires privacy policies to include information on how the operator responds to Do Not Track signals or similar mechanisms; the law also now requires privacy policies to state whether third parties can collect personally identifiable information about the site's users.[36]

As a result, many organizations have implemented specialized software to track and record compliance actions, hired management consultants to provide advice and training on compliance issues, and even created a new position, the chief compliance officer (CCO), to deal with compliance-related issues.

In 1972, the SEC recommended that publicly held organizations establish audit committees.[37] The **audit committee** of a board of directors provides assistance to the board in fulfilling its responsibilities with respect to the oversight of the following areas of activity:

- The quality and integrity of the organization's accounting and reporting practices and controls, including financial statements and reports
- The organization's compliance with legal and regulatory requirements

- The qualifications, independence, and performance of the company's independent auditor (a certified public accountant who provides a company with an accountant's opinion but who is not otherwise associated with the company)
- The performance of the company's internal audit team

In some cases, audit committees have uncovered violations of law and have reported their findings to appropriate law enforcement agencies.

Marvell Technology Group LTD is a Silicon Valley-based producer of semiconductors and related products. In early 2016, the firm launched an audit committee investigation that scrutinized financial results for several quarters. The audit committee uncovered that in some cases Marvell personnel, IT users, would ask customers to accept delivery of products sooner than they had requested allowing the company to book revenue in earlier quarters. Such transactions were made in response to "significant pressure" from the management on sales teams to meet revenue targets. Such sales reporting accounted for about 9 percent of first quarter revenue in fiscal 2016 and 11 percent for the second quarter. Facing pressure from investors, both the firm's chief executive and its president were fired. In their first conference call with investors, the firm's new management team pledged to discontinue the practice of booking revenue prematurely.[38]

In addition to an audit committee, most organizations also have an internal audit department whose primary responsibilities include the following:

- Determine that internal systems and controls are adequate and effective
- Verify the existence of company's assets and maintain proper safeguards over their protection
- Measure the organization's compliance with its own policies and procedures
- Ensure that institutional policies and procedures, appropriate laws, and good practices are followed
- Evaluate the adequacy and reliability of information available for management decision making

Although the members of the internal audit team are not typically experts in detecting and investigating financial statement fraud, they can offer advice on how to develop and test policies and procedures that result in transactions being recorded in accordance with generally accepted accounting principles (GAAP). This can go a long way toward deterring fraud related to an organization's financial statements. Quite often in cases of financial statement fraud, senior management (including members of the audit committee) ignored or tried to suppress the recommendations of the internal audit team, especially when red flags were raised.

CRITICAL THINKING EXERCISE: CREATING AN AUP

You are a new member of the infosec group for a midsized consumer products manufacturing organization. After you have been there a few weeks, you are shocked to learn that the organization has not defined an AUP. You are determined to prioritize the creation of such a policy for the infosec group. What key points can you make to management to justify the necessary time and effort to create an AUP? Who else should you recruit in your efforts to sell this idea to management? Identify the key points that should be included in the AUP.

Summary

What relationships must an IT worker manage, and what key ethical issues can arise in each?

- An IT worker must maintain good working relationships with employers, clients, suppliers, other professionals, IT users, and society at large. Each relationship has its own set of ethical issues and potential problems.
- In relationships between IT workers and employers, important issues include setting and enforcing policies regarding the ethical use of IT, the potential for whistle-blowing, and the safeguarding of trade secrets.
- In relationships between IT workers and clients, key issues revolve around defining, sharing, and fulfilling each party's responsibilities for successfully completing an IT project. The IT worker must remain objective and guard against any sort of conflict of interest, fraud, misrepresentation, or breach of contract.
- A major goal for IT workers and suppliers is to develop good working relationships in which no action can be perceived as unethical.
- Bribery is the act of providing money, property, or favors to someone in business or government in order to obtain a business advantage.
- Internal control is the process established by an organization's board of directors, managers, and IT group to provide reasonable assurance for the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations.
- Policies are the guidelines, standards, and laws by which the organization must abide. Policies drive processes and procedures. Processes are a collection of tasks designed to accomplish a stated objective. A procedure defines the exact instructions for completing each task in a process.
- A fundamental concept of good internal control is the careful separation of duties associated with any process that involves the handling of financial transactions so that different aspects of the process are handled by different people.
- The Foreign Corrupt Practices Act (FCPA) makes it a crime to bribe a foreign official, a foreign political party official, or a candidate for foreign political office. The act applies to any U.S. citizen or company and to any company with shares listed on any U.S. stock exchange.
- In relationships between IT workers and other professionals, the priority is to improve the profession through activities such as mentoring inexperienced colleagues, demonstrating professional loyalty, and avoiding résumé inflation and the inappropriate sharing of corporate information.
- In relationships between IT professionals and IT users, important issues include software piracy, inappropriate use of IT resources, and inappropriate sharing of information.
- When it comes to the relationship between IT workers and society at large, the main challenge for IT workers is to practice the profession in ways that cause no harm to society and provide significant benefits.

What can be done to encourage the professionalism of IT workers?

- A professional is one who possess the skill, good judgment, and work habits expected from a person who has the training and experience to do a job well.
- A professional is expected to contribute to society, to participate in a lifelong training program, to keep abreast of developments in the field, and to help develop other professionals.
- IT workers of all types can improve their profession's reputation for professionalism by (1) subscribing to a professional code of ethics, (2) joining and participating in professional organizations, (3) obtaining appropriate certifications, and (4) supporting government licensing where available.
- A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group.
- Codes of ethics usually have two main parts—the first outlines what the organization aspires to become and the second typically lists rules and principles that members are expected to live by. The codes also typically include a commitment to continuing education for those who practice the profession.
- Adherence to a code of ethics can produce many benefits for the individual, the profession, and society as a whole, including ethical decision making, high standards of practice and ethical behavior, trust and respect with the general public, and access to an evaluation benchmark that can be used for self-assessment.
- Several IT-related professional organizations have developed a code of ethics, including ACM, IEEE-CS, AITP, and SANS.
- Many people believe that the licensing and certification of IT workers would increase the reliability and effectiveness of information systems.
- Certification indicates that a professional possesses a particular set of skills, knowledge, or abilities, in the opinion of the certifying organization. Numerous companies and professional organization offer certification.
- Most states support the licensing of software engineers, and the state licensing boards have ultimate responsibility over specific requirements for licensing in their jurisdiction.

What ethical issues do IT users face, and what can be done to encourage their ethical behavior?

- IT users face several common ethical issues, including software piracy, inappropriate use of computing resources, and inappropriate sharing of information.
- Actions that can be taken to encourage the ethical behavior of IT users include establishing guidelines for the use of company hardware and software; defining an AUP for the use of IT resources; structuring information systems to protect data and information; installing and maintaining a corporate firewall; and ensuring compliance with laws, policies, and standards.
- The information security (infosec) group is responsible for managing the processes, tools, and policies necessary to prevent, detect, document, and counter threats to digital and nondigital information.
- The audit committee of a board of directors and members of the internal audit team have a major role in ensuring that both the IT organization and IT users are in compliance with organizational guidelines and policies as well as various legal and regulatory practices.

Key Terms

acceptable use policy (AUP)
audit committee
body of knowledge
breach of contract
breach of the duty of care
bribery
BSA | The Software Alliance (BSA)
certification
compliance
conflict of interest
duty of care
firewall
Foreign Corrupt Practices Act (FCPA)
fraud
government license
information security (infosec) group
internal control
IT user
material breach of contract
misrepresentation
negligence
policy
procedure
process
professional code of ethics
professional malpractice
reasonable person standard
reasonable professional standard
résumé inflation
separation of duties
Software & Information Industry Association (SIIA)
software engineer
trade secret
whistle-blowing

Self-Assessment Questions

What relationships must an IT worker manage, and what key ethical issues can arise in each?

1. An IT worker cannot be sued for professional malpractice unless he or she is licensed. True or False.

2. The mission of the Software & Information Industry Association and the Business Software Alliance is to ______________.
   a. protect the trade secrets of world's largest software and hardware manufacturers
   b. encourage disgruntled employees to report misdeeds by their employers
   c. stop the unauthorized copying of software produced by its members
   d. provide recommendations on how to develop software code that is unhackable

3. ______________ is an effort by an employee to attract attention to a negligent, illegal, unethical, abusive, or dangerous act by a company that threatens the public interest.

4. ______________ occurs when a party fails to perform certain express or implied obligations, which impairs or destroys the very essence of a contract.
   a. Fraud
   b. Material breach of contract
   c. Breach of contract
   d. Misrepresentation
5. Under the Foreign Corrupt Practices Act (FCPA), it is permissible to pay an official to perform some official function faster (for example, to speed customs clearance). True or False.

What can be done to encourage the professionalism of IT workers?

6. A(An) ______________ states the principles and core values that are essential to the work of a particular occupational group.
7. Unlike certification, which applies only to people and is required by law, licensing can also apply to products. True or False.
8. To become licensed as a software engineer in the United States, one must pass the Fundamental of Engineering exam and a software engineering ______________ exam.
9. The core ______________ for any profession outlines agreed-upon sets of skills and abilities that all licensed professionals must possess.
10. Professionals who breach the duty of care are liable for injuries that their negligence causes. This liability is commonly referred to as ______________.
    a. negligence
    b. professional malpractice
    c. breach of contract
    d. breach of contract
11. Senior management (including members of the audit committee) must always follow the recommendations of the internal audit committee. True or False.
12. ______________ is the process established by an organization's board of directors, managers, and IT systems people to provide reasonable assurance for the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations.

What ethical issues do IT users face, and what can be done to encourage their ethical behavior?

13. The software piracy rates in Albania, Kazakhstan, Libya, Panama, and Zimbabwe ______________.
    a. exceed 90 percent
    b. are nearly 100 percent
    c. exceed 70 percent
    d. are about 50 percent

14. Which of the following is *not* one of the five key elements of an acceptable use policy (AUP)?
    a. Purpose of the AUP, why it is needed and what are its goals
    b. Background and make-up of the infosec organization that enforces the AUP
    c. Definition of the actions that will be taken against an individual who violates the policy
    d. Scope of who and what is covered under the AUP

15. A ____________ is hardware or software (or a combination of both) that serves as the first line of defense between an organization's network and the Internet; it also limits access to the company's network based on the organization's Internet-usage policy.

Self-Assessment Answers

1. True; 2. c; 3. Whistle-blowing; 4. b; 5. True; 6. professional code of ethics or code of ethics; 7. False; 8. Principles and Practices; 9. body of knowledge; 10. b; 11. True; 12. Internal control; 13. c; 14. b; 15. firewall

Discussion Questions

1. What characteristics would you say are true earmarks of an employee who is unprofessional in his or her approach to work?
2. How do you distinguish between breach of contract and material breach of contract? Provide an example of a breach of contract that would not be a material breach of contract.
3. When companies are filling open positions in U.S.-based IT organizations, do you think that preference should be shown for qualified candidates from the United States over qualified candidates from foreign countries? Why or why not?
4. Does your employer or school have an acceptable use policy in place? Are you familiar with it? Were you asked to sign it?
5. Review the Software Engineering Code of Ethics and Professional Practice presented in Figure 2-3. Identify and briefly describe a ninth principle that you feel should be added to this code.
6. Describe a situation in which there could be a conflict of interest between an IT consultant's self-interest and the interests of a client. How might this potential conflict be addressed?
7. Should software developers who work on critical applications whose failure could result in loss of human life (for example, software for self-driving cars) be required to be licensed? Why or why not?
8. Review the acceptable use policy prepared by the SANS Institute (https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy). Is this code clear and concise? Does it provide a strong justification for following the AUP? Does it specify sanctions that will be enacted for violation of the AUP? What necessary changes do you feel should be made?

9. What do you think are the benefits you can derive from joining a professional organization for people in your chosen career field? If you were to join one professional organization, which one would it be?
10. The Foreign Corrupt Practices Act (FCPA) allows a bribe to be made under what conditions? Explain, and provide an example.
11. What certifications are available for someone in your chosen career field? Which of these are considered most valuable?
12. What is the difference between a breach of duty of care and professional malpractice?

What Would You Do?

Use the five-step decision-making process discussed in Chapter 1 to analyze the following situations and recommend a course of action.

1. You are a CPA and have been asked to volunteer a few hours of your time to review the accounting records and procedures of a small nonprofit, charitable organization with an annual budget just under $5 million. During your review, you are surprised to find accounting records indicating that the CFO initiated and approved three non-payroll checks totaling $10,500 made out to one of the organization's employees. During the course of a private conversation with the CFO, you learn that she "loaned" the money to an employee with 15 years of service whose teenage son is fighting heroin addiction. The nonprofit's insurance does not provide any benefits to cover the cost of addiction treatment. The employee has promised to pay the money back over time after he gets back on his feet financially. What do you do? Do you include this finding in your audit report?
2. You are a new human resources manager assigned to your firm's IT organization. One of your responsibilities is to screen résumés for job openings in the IT organization. You are in the process of reviewing more than 35 résumés you received for a position as a Cisco network specialist. Your goal is to trim the group down to the top five candidates to invite to an in-house interview. About half the résumés are from IT workers with less than three years of experience who claim to have one or more Cisco certifications. There are also a few candidates with over five years of impressive experience but who have no Cisco certifications listed on their résumés. You were instructed to include only candidates with a Cisco certification in the list of finalists. However, you are concerned about possible résumé inflation and the heavy emphasis on certification versus experience. What would you do?
3. You are a new salesperson at a large software manufacturing firm. It is three weeks from the end of the sales quarter and you and your sales manager have both already met your sales quotas for the quarter. In addition, you just closed another deal with a new customer for $100,000 worth of software and customer service. This order would put you way over your sales quota for the current quarter. Your manager suggests that you hold this new order so it gets recorded against next quarter. She explains that because sales during the next three months tend to slow down, salespeople frequently miss their quotas and associated sales bonuses for that quarter. Holding this large order to next quarter would help you get an excellent start and almost guarantee that you meet your quota. What would you do?

4. You are caught in the middle of a dilemma. You have been subpoenaed to be a witness in a work-related sexual harassment case involving your boss and a coworker. On more than one occasion, you heard your boss make statements to this employee that could be interpreted as sexual advances. Your boss has made it clear that he will make things difficult for you at work if you testify in favor of the employee. You could choose to testify in a manner that would make it appear that your boss was not serious and that the employee was overreacting. However, you truly thought that your boss was not joking with the employee and that he was harassing her. What kind of repercussions could there be if you testify in favor of your coworker? Would you be willing to risk those repercussions?
5. Your old roommate from college was recently let go from his firm during a wave of employee terminations to reduce costs. You two have kept in touch over the six years since school, and he has asked you to help him get a position in the IT organization where you work. You offered to review his résumé, make sure that it gets to the "right person," and even put in a good word for him. However, as you read the résumé, it is obvious that your friend has greatly exaggerated his accomplishments at his former place of work and even added some IT-related certifications you are sure he never earned. What would you do?
6. You are in charge of awarding all computer hardware service contracts (valued at over $2 million per year) for your employer. In recent emails with the company's current service contractor, you casually mentioned that you were looking to buy a new car and that you really liked the Audi automobile, but it was very expensive. You are surprised when the contractor texts you the name of the sales manager at a local Audi dealer and suggests you give him a call. The contractor says the owner of the dealership is a good friend and he will be able to give you a great deal on a new Audi. If your manager saw a copy of the texts exchanged with the contractor, could it appear that you were soliciting a bribe? Could this offer be considered a bribe? What would you do?

Cases

1. Bridgestone versus IBM

Bridgestone Americas, Inc., a subsidiary of the Japan-based Bridgestone Group, is a provider of tires and rubber-related products and services with operations in North and South America. Bridgestone North American is a major tire supplier in the United States, and on average, its customers submit one product order per second, eight hours per day, five days a week. In order to process such a high volume of orders, Bridgestone requires front- and back-office systems that work together seamlessly.

To meet that goal, Bridgestone contracted with IBM in 2009 to replace its legacy information systems using software from SAP (one of the world's largest software suppliers) to automate and accelerate the entire order-to-cash process. This process is considered the lifeline of any organization as it supports the tasks associated with order entry, order fulfillment, order shipment, invoicing, customer payment, and cash application to general ledger. Under the contract, IBM agreed to develop necessary new programs and implement a new system in such a manner that it integrated with other Bridgestone software.

The project, which ran from 2009 to early 2012, was both large and complex. Ultimately, IBM charged Bridgestone almost $80 million for its services on this project—$30 million over budget. The system went live in January 2012, five months behind schedule, with all aspects of the system “going live” simultaneously across all of Bridgestone’s North American tire operations. According to IBM, this high risk flash cutover was done only at Bridgestone’s insistence, over IBM’s objections that the system was not ready. IBM also alleged that one reason the system was not ready is that Bridgestone failed to fulfill certain contractual obligations.

According to Bridgestone, the launch was a disaster. The system lost scheduled customer orders, would not process some orders, and duplicated or partially processed other orders. In addition, critical follow-up actions were not completed for the few orders that the system did initially process.

In an effort to more quickly resolve the critical issues that arose after the system launched, Bridgestone chose to hire SAP directly to fix the many problems. IBM’s work in the months following the launch was focused on fixing problems in the programs it had written; unfortunately, according to Bridgestone, IBM’s failed troubleshooting work often resulted in new problems.

In late 2013, Bridgestone filed suit against IBM in federal court in Nashville, Tennessee, alleging breach of contract, fraud, gross negligence, and misrepresentation on the part of IBM. Bridgestone is also pursuing claims under the Tennessee Consumer Protection Act. The tire company is seeking treble damages ($600 million) from IBM. Bridgestone claims it incurred more than $200 million in lost sales and additional costs as a result of the faulty implementation. Bridgestone also alleges that it relied on misrepresentations by IBM to award it the contract for this work. In addition, Bridgestone contends that IBM concealed and/or negligently failed to disclose material facts regarding the implementation of the system that would have resulted in different decisions regarding the project. Bridgestone further complained that the system was not sufficiently advanced to meet its needs and that IBM had assigned personnel lacking the necessary skills and experience to the project.

For its part, IBM claims that Bridgestone failed to provide the necessary leadership for the project, asserting that the tire company replaced its CIO six times during the course of the project and failed to staff the project with employees who sufficiently understood its own legacy systems. In addition, IBM pointed out that the project had been attempted with other vendors who had failed to upgrade the system and that IBM had been called in to rescue the project. IBM also claimed that Bridgestone had refused to do necessary testing prior to the system going live and that IBM had strongly recommended that the system launch be delayed until known bugs were fixed. IBM said it had made some concessions to Bridgestone for some problems that came up during the project and that Bridgestone had signed a release absolving IBM of responsibility.

It is highly unusual for two companies in such a dispute to make their issues so public as it results in bad public relations for both firms. Legal expenses and employee time and effort are expected to be quite high for both sides in this case. During pretrial discovery, Bridgestone turned over 1.6 million documents related to the case. Each side is permitted to present 30 expert witnesses who can be disposed for up to seven hours each.

Critical Thinking Questions

1. With 20-20 hindsight, what could each side have done differently to improve the outcome of this major project?

2. Which company's reputation was harmed more by the publicity surrounding this project? What might have been done to better protect this company's reputation?
3. At the time of this writing, the case has not been decided. Do research online to find out how things turned out.

Sources: *Bridgestone Americas, Inc. v. International Business Machines Corporation*, United States District Court, Middle District of Tennessee, Nashville Division No. 3:13-1196, http://law.justia.com/cases/federal/district-courts/tennessee/tnmdce/3:2013cv01196/57186/352/ (accessed September 7, 2016); J.R. Lind, "Bridgestone Files Massive Fraud and Deception Suit Against IBM," *Nashville Post*, November 18, 2013, www.nashvillepost.com/business/legal/article/20473190/bridgestone-files-massive-fraud-and-deception-suit-against-ibm; Julie Bort, "IBM Rips into Bridgestone Over $600 Million Lawsuit," *Business Insider*, November 20, 2013, www.businessinsider.com/ibm-rips-into-bridgestone-over-600-million-lawsuit-2013-11; John Belden, "Bridgestone to IBM: Don't Tread on Me! 6 Lessons to Learn," *Upper Edge*, January 7, 2014, http://upperedge.com/sap/bridgestone-to-ibm-dont-tread-on-me-6-lessons-to-learn; John Belden, "IBM's Implementation of SAP Bridgestone: Don't Tread on Me Update," *Upper Edge*, October 6, 2015, http://upperedge.com/sap/ibms-implementation-of-sap-at-bridgestone-dont-tread-on-me-update/; "Judge Dismisses Part of Bridgestone Lawsuit Against IBM," *Nashville Post*, March 28, 2016, www.nashvillepost.com/business/legal/article/20492360/judge-dismisses-part-of-bridgestone-lawsuit-against-ibm.

2. SAP Found in Violation of FCPA

SAP is a software company based in Hanover, Germany, that sells software licenses and related services to over 320,000 customers in 190 countries. It employs some 79,000 workers and works with more than 12,000 partner companies worldwide. In 2015, the company reported revenue of $23.2 billion.

In order to generate and sustain such high levels of income, SAP, along with many other IT companies, employs a complex set of consultants, distributors, retailers, systems integrators, technology deployment consultancies, value-added resellers, and vendors to market and sell their products and services. The use of so many entities increases the possibility that someone in the distribution chain might engage in bribery, putting the company at risk. IT companies such as SAP are challenged to build a constantly vigilant monitoring program and must spend significant resources to guard against such illegal actions, including those that could be prosecuted under the Foreign Corrupt Practices Act (FCPA). In recent years, a number of IT companies have been the subject of FCPA enforcement actions including Cisco, Hewlett-Packard, IBM, and Oracle, just to name a few. Even though SAP is a German company, it is also subject to the FCPA because its shares are traded on the New York Stock Exchange.

The former vice president of global and strategic accounts for SAP conspired with four members of the SAP distribution chain to pay bribes to Panamanian government officials to secure a major technology upgrade contract. The contract was for $14.5 million, including $2.1 million in software licenses for SAP. The Panamanian government subsequently awarded SAP's distribution partner further contracts that included SAP products worth an additional $1.2 million. The SAP executive paid $145,000 in bribes to one government official, and he himself took over $85,000 in kickbacks for arranging the bribes.

The bribes were paid through bogus contracts and false invoices, with funds obtained by SAP selling the software to one of its distributors at a deep discount—over 80 percent in some cases. The software was then sold to the Panamanian government at a much higher price. The difference between the higher price paid by the Panamanian government and the discounted price paid by the distribution partner created a slush fund that the partner used to pay the bribes and kickbacks. The deep discounts were falsely reported as legitimate discounts on the books of SAP's Mexican subsidiary and were subsequently consolidated into SAP's financial statements.

SAP's system of internal control required employees to submit requests within SAP to obtain approval of discounts to local partners. SAP employees, however, had wide latitude in seeking and approving such discounts. So although the deep discounts should have triggered additional scrutiny, they did not; the employees' explanations for the discounts were accepted without verification.

The Securities and Exchange Commission (SEC) charged the SAP executive with violation of the Foreign Corrupt Practices Act (FCPA), and he was forced to pay $92,000, representing the amount of the kickback he received on the deal plus interest. He was also sentenced to 22 months in prison.

According to the SEC, the illegal activity went undetected because SAP failed to devise and maintain a system of internal accounting controls adequate to provide reasonable assurances that these improper payments to government officials did not occur. The SEC fined SAP $3.9 million to settle charges that it violated the internal control provision and the books and records provision of the FCPA. This amount represented the $3.7 million in profits SAP earned on the contracts plus another $.2 million in interest. SAP agreed to pay the $3.9 million fine without admitting or denying the SEC's findings.

Critical Thinking Questions

1. Do you think that the penalty for violation of the internal control provision and the books and records provision of the FCPA is stiff enough to motivate companies to implement systems capable of detecting bribes? Is it possible that some organizations tolerate lax internal control so managers have as much freedom as possible in running their business? What changes, if any, would you suggest to the FCPA?
2. When an organization implements a major accounting software package, it also inherits the system of internal control that is built into the software—good, bad, or indifferent. What can be done if it is discovered, months after the software has been purchased and installed, that the software is lacking in good internal control?
3. IT workers have a key role in designing and implementing the internal controls associated with systems that automate the processing of business transactions, such as the payment of suppliers, employees, and business partners and the receipt of payments from customers. What can IT workers do to prepare themselves for this responsibility? Who should the IT workers collaborate with when evaluating or designing the automated internal controls of a computer-based information system?

Sources: "Company Information," SAP SE, http://go.sap.com/corporate/en/company.fast-facts.html (accessed October 18, 2016); "Press Release: SEC Charges Former Software Executive with FCPA Violations," U.S. Securities and Exchange Commission, August 12, 2015, https://www.sec.gov/news/pressrelease/2015-165.html; "Former Executive Pleads Guilty to Conspiring to Bribe Panamanian Officials," Department of Justice, Office of Public Affairs, August 12, 2015, https://www.justice.gov/opa/pr/former-executive-pleads-guilty-conspiring-bribe-panamanian-officials; Richard L. Cassin, "Former SAP

Exec Jailed 22 Months for Panama Bribes," *The FCPA Blog*, December 17, 2015, www.fcpablog.com/blog/2015/12/17/former-sap-exec-jailed-22-months-for-panama-bribes.html; Richard L. Cassin, "SAP Settles Panama Bribes Case with SEC for $3.9 Million," *The FCPA Blog*, February 1, 2016, www.fcpablog.com/blog/2016/2/1/sap-settles-panama-bribes-case-with-sec-for-39-million.html; "2016 FCPA Enforcement Begins with SEC Action Against SAP," *FCPA Professor*, February 2, 2016, http://fcpaprofessor.com/2016-fcpa-enforcement-begins-with-sec-action-against-sap/.

End Notes

[1] Julie Bort, "IBM Sued Over $1 Billion Project That Led to It Being Banned by Queensland, Australia," *Business Insider*, December 7, 2013, www.businessinsider.com.au/queensland-sues-ibm-over-1b-project-2013-12.

[2] "Queensland Government to Sue IBM Over Health Payroll Disaster," *Australian*, December 1, 2014, www.theaustralian.com.au/business/technology/queensland-government-to-sue-ibm-over-health-payroll-disaster/news-story/bd9ef745151d6708b8dcd19f24161d28.

[3] "BSA Survey: Unlicensed Software Use Still High Globally, Despite Costly Cybersecurity Threats," BSA, www.bsa.org/news-and-events/news/2016/may/05252016globalsoftwaresurvey (accessed May 25, 2016).

[4] "Compliance and Enforcement Focused Communications," http://www.bsa.org/anti-piracy/ap-communications (accessed October 20, 2016).

[5] "About SIIA," http://www.siia.net/About/About-SIIA (accessed October 20, 2016).

[6] "BSA Global Enforcement," http://www.bsa.org/anti-piracy/enforcement (accessed October 20, 2016).

[7] Robert J. Scott, "Software Piracy Claims Can Ruin Your Business and Reward Those Responsible," May 10, 2016, https://techcrunch.com/2016/05/10/software-piracy-claims-can-ruin-your-business-and-reward-those-responsible/.

[8] Graham Wood "Sanctions for Zillow in Move Lawsuit?" *RealtorMag*, April 26, 2016, http://realtormag.realtor.org/daily-news/2016/04/26/sanctions-for-zillow-in-move-lawsuit.

[9] Ben Lane, "Zillow to Pay $130M to Settle Lawsuit with Move Over Alleged Trade Secret Theft," *Housing Wire*, June 6, 2016, www.housingwire.com/articles/37204-zillow-to-pay-130m-to-settle-lawsuit-with-move-over-alleged-trade-secret-theft.

[10] Sarah McBride, "Oracle Whistleblower Suit Raises Questions Over Cloud Computing," *Reuters*, June 6, 2016, www.reuters.com/article/us-oracle-lawsuit-accounting-idUSKCN0YS0X1.

[11] Julie Bort, "Oracle Says It Will Sue Fired Employee Who Filed a 'Whistleblower' Lawsuit," *Business Insider*, June 2, 2016, www.businessinsider.com/oracle-says-will-sue-fired-whistleblower-employee-2016-6.

[12] Dan Goodin, "Security Firm Sued for Filing 'Woefully Inadequate' Forensics Report," *Arstechnica,* January 15, 2016, http://arstechnica.com/security/2016/01/security-firm-sued-for-filing-woefully-inadequate-forensics-report/.

[13] Henry R. Cheeseman, "Contemporary Business Law," 3rd ed. (Upper Saddle River, NJ: Prentice Hall, 2000), 292.

[14] Peter Bright, “HP Awarded $3B in Damages from Oracle Over Itanium Database Cancellation,” *Arstechnica*, June 30, 2016, http://arstechnica.com/information-technology/2016/06/hp-awarded-3b-in-damages-from-oracle-over-itanium-database-cancellation/.

[15] Agence France-Presse, “Former Foxconn Employees Indicted for Bribery,” *IndustryWeek*, May 22, 2014, www.industryweek.com/supplier-relationships/former-foxconn-employees-indicted-bribery.

[16] Adrian Krajewski and Aruna Viswanatha, “HP Pays $108 Million to Settle Foreign Bribery Probes,” *Reuters*, April 9, 2014, www.reuters.com/article/us-poland-hp-idUSBREA380EZ20140409.

[17] Jack Nickas, “What Is Yahoo? Riddle Plagued CEOs for Two Decades,” *Wall Street Journal,* July 25, 2016, www.wsj.com/articles/what-is-yahoo-riddle-plagued-ceos-for-two-decades-1469446207.

[18] “Hiring Smart: How to Avoid the Top Ten Mistakes,” Ropella, www.ropella.com/index.php/knowledge/recruitingProcessArticles/hiring_smart (accessed October 17, 2016).

[19] Patrick Foster, “UKTV Executive Sacked after Stealing Huge Cache of Confidential TV Data from Media Regulator,” *The Telegraph*, March 16, 2016, www.telegraph.co.uk/news/media/12196109/UKTV-executive-sacked-after-stealing-huge-cache-of-confidential-TV-data-from-media-regulator.html.

[20] “ACM History,” ACM, www.acm.org/about-acm/acm-history (accessed October 17, 2016).

[21] “About the ACM Organization,” Association for Computing Machinery, https://www.acm.org/about-acm/about-the-acm-organization (accessed August 28, 2016).

[22] “About IEEE-CS,” IEEE, https://www.computer.org/web/about/history (accessed August 28, 2016).

[23] “History of AITP,” AITP, www.aitp.org/?page=AITPHistory (accessed August 28, 2016).

[24] “About SANS,” SANS, https://www.sans.org/about/ (accessed August 28, 2016).

[25] Association of Computing Machinery, “Software Engineering Code of Ethics and Professional Practice,” https://www.acm.org/about/se-code (accessed September 14, 2016).

[26] “About NCEES”, http://ncees.org/about (accessed October 17, 2016).

[27] “NCEES Principles and Practice of Engineering Examination: Software Engineering Exam Specifications,” NCEES, http://ncees.org/wp-content/uploads/2015/07/SWE-Apr-2013.pdf (accessed October 17, 2016).

[28] “Lebanon’s Software Piracy Rate as High as China’s: US Report,” *Albawaba*, May 30, 2016, www.albawaba.com/business/lebanons-software-piracy-rate-high-chinas-us-report-846208.

[29] Dave Smith, “Android Still Has a Massive Piracy Problem,” *Business Insider*, January 8, 2015, www.businessinsider.com.au/android-piracy-problem-2015-1.

[30] Andres Millington, “Porn in the Workplace Is Now a Major Board-Level Concern for Business,” *Business Computing World*, April 23, 2010.

[31] Dean Wilson, “Third of Mobile Workers Distracted by Porn, Report Finds,” *TechEYE.net*, June 14, 2010.

[32] Associated Press, “WikiLeaks Reveals Sensitive Diplomacy,” *Cincinnati Enquirer*, November 28, 2010.

[33] Justin Baer, “Morgan Stanley Fires Employee Over Client-Data Leak,” *Wall Street Journal*, January 5, 2015, www.wsj.com/articles/morgan-stanley-terminates-employee-for-stealing-client-data-1420474557.

[34] Matt Robinson, “Morgan Stanley Fined Over Lapses Tied to Adviser’s Data Breach,” *Bloomberg Technology*, https://www.bloomberg.com/news/articles/2016-06-08/morgan-stanley-to-pay-sec-fine-tied-to-adviser-s-data-breach.

[35] Matthew J. Schwartz, “California Targets Mobile Apps for Missing Privacy Policies,” *InformationWeek*, October 31, 2012.

[36] Gregory S. McNeal, “California AG Releases Guide to Online Privacy Laws,” *Forbes*, May 21, 2014, www.forbes.com/sites/gregorymcneal/2014/05/21/california-ag-releases-guide-to-californias-online-privacy-laws/#48be5b8f4e72.

[37] Annemarie K. Keinath and Judith C. Walo, “Audit Committee Responsibilities,” *The CPA Journal Online*, http://archives.cpajournal.com/2004/1104/essentials/p22.htm (accessed August 30, 2016).

[38] Don Clark and Maria Armental, “Marvell’s Quarterly Profit Drops Sharply; Chip Maker Posts Annual Loss,” *Wall Street Journal*, July 19, 2016, www.wsj.com/articles/marvells-quarterly-profit-drops-sharply-chip-maker-posts-annual-loss-1468965888.

CHAPTER 3

CYBERATTACKS AND CYBERSECURITY

QUOTE

Most people are starting to realize that there are only two different types of companies in the world: those that have been breached and know it and those that have been breached and don't know it. Therefore, prevention is not sufficient, and you're going to have to invest in detection because you're going to want to know what system has been breached as fast as humanly possible so that you can contain and remediate.

—Ted Schlein, Venture capitalist focusing on networking and consumer security

Lagarto Film/Shutterstock.com

ORGANIZATIONS BEHAVING BADLY

A **zero-day exploit** is a cyberattack that takes place before the security community and/or software developers become aware of and fix a security vulnerability. It takes advantage of security flaws that enable unauthorized users to gain access to a computer system or to download sensitive user data. Until a zero-day exploit is discovered and a patch is written to fix the underlying flaw, users of the software are vulnerable to attack. Zero-day exploits have been found in widely used software such as Acrobat Reader, Adobe Flash Player, Apple iOS, Google Chrome, Java, Microsoft Internet Explorer, and Microsoft Windows.

While one would hope that the discoverer of a zero-day vulnerability would immediately inform the original software manufacturer so that a fix can be created for the problem, unfortunately this is often not the case. In some cases, this knowledge is sold on the black market to hackers, cyberterrorists, governments, or large organizations that may then use it to launch their own cyberattacks. Information about one zero-day vulnerability in Apple's iOS was reportedly sold for $500,000.[1]

The U.S. Federal Bureau of Investigation, Department of Defense, National Security Agency, and other government agencies spend heavily on information about vulnerabilities in computer systems. Packages of zero-day exploits have reportedly been sold to U.S. government contractors for $2.5 million a year.[2] In many cases, these agencies choose not to inform the public about such cyber threats, leaving all users of the affected software vulnerable to attack. The reasoning behind such an approach is that keeping a zero-day vulnerability secret from others allows these intelligence and law enforcement agencies to create a powerful tool that can be wielded for espionage or cyberattack purposes.

In theory, U.S. agencies are not allowed to withhold "major" cybersecurity vulnerabilities from the companies affected by them, with few exceptions, under a policy known as the Vulnerability Equities Process (VEP). However, critics argue that this policy is not transparent (for instance, it is not clear what triggers the VEP or how many cybersecurity vulnerabilities have been disclosed to affected organizations).[3] Under VEP, the Federal Bureau of Investigation (FBI) found an exception that allowed it to refuse to reveal the vulnerability that enabled it to hack into the iPhone of the San Bernardino shooter who killed 14 people in late 2015. In addition, because the VEP is an executive branch administrative policy—not a law or executive order—it can be overturned at any time by the president.[4,5,6]

What trade-offs must be considered by these government agencies in deciding which zero-day exploits should be publicized and which should be kept secret? Are these agencies acting in the best interests of its citizens in this regard?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. Why are computer incidents so prevalent, and what are their effects?
2. What can be done to implement a strong security program to prevent cyberattacks?
3. What actions must be taken in the event of a successful security intrusion?

THE THREAT LANDSCAPE

The security of data and information systems used in business is of utmost importance. Confidential business data and private customer and employee information must be safeguarded, and systems must be protected against malicious acts of theft or disruption. Although the need for security is obvious, it must often be balanced against other business needs. Business managers, IT professionals, and IT users all face a number of complex trade-offs when making decisions regarding IT security, such as the following:

- How much effort and money should be spent to safeguard against computer crime? (In other words, how safe is safe enough?)
- What should be done if recommended computer security safeguards make conducting business more difficult for customers and employees, resulting in lost sales and increased costs?
- If a firm is a victim of a cybercrime, should it pursue prosecution of the criminals at all costs, maintain a low profile to avoid the negative publicity, inform affected customers, or take some other action?

The number of cybercrimes being committed against individuals, organizations, and governments continues to grow, and the destructive impact of these crimes is also intensifying. The brands, reputation, and earnings of many organizations around the world have been negatively impacted by such crimes. As a result, organizations are putting in place a range of countermeasures to combat cybercrime. For instance, the worldwide financial services industry spent $27.4 billion on IT security and fraud prevention in 2015.[7] And a recent survey of more than 10,000 IT professionals around the world revealed the following:[8]

- 58 percent of global companies have an overall security strategy
- 54 percent have a chief information security officer (CISO) in charge of security

- 53 percent have employee security awareness and training programs
- 52 percent have security standards for third parties
- 49 percent conduct threat assessments
- 48 percent actively monitor and analyze security intelligence

In spite of all these countermeasures, however, the number of computer security incidents surged from 2014 to 2015 in the following industries: public sector organizations; entertainment, media, and communications; technology and telecommunications companies; pharmaceuticals and life sciences; and power and utilities organizations.[9]

Why Computer Incidents Are So Prevalent?

Increasing computing complexity, expanding and changing systems, an increase in the prevalence of bring your own device (BYOD) policies, a growing reliance on software with known vulnerabilities, and the increasing sophistication of those who would do harm have caused a dramatic increase in the number, variety, and severity of security incidents.

Increasing Complexity Increases Vulnerability

Computing environments have become enormously complex. Cloud computing, networks, computers, mobile devices, virtualization, operating systems, applications, websites, switches, routers, and gateways are interconnected and driven by hundreds of millions of lines of code. This environment continues to increase in complexity every day. The number of possible entry points to a network expands continually as more devices are added, increasing the possibility of security breaches.

Expanding and Changing Systems Introduce New Risks

Business has moved from an era of stand-alone computers, in which critical data were stored on an isolated mainframe computer in a locked room, to an era in which personal computers and mobile devices connect to networks with millions of other computers, all capable of sharing information. Businesses have moved quickly into e-commerce, mobile computing, collaborative work groups, global business, and interorganizational information systems. Information technology has become ubiquitous and is a necessary tool for organizations to achieve their goals. However, it is increasingly difficult for IT organizations to keep up with the pace of technological change, successfully perform an ongoing assessment of new security risks, and implement approaches for dealing with them.

Increasing Prevalence of BYOD Policies

Bring your own device (BYOD) is a business policy that permits, and in some cases encourages, employees to use their own mobile devices (smartphones, tablets, or laptops) to access company computing resources and applications, including email, corporate databases, the corporate intranet, and the Internet. Proponents of BYOD say it improves employee's productivity by allowing workers to use devices with which they are already familiar—while also helping to create an image of a company as a flexible and progressive employer.

Most companies have found they cannot entirely prevent employees from using their own devices to perform work functions. However, this practice raises many potential security issues as it is highly likely that such devices are also used for nonwork activity (browsing websites, shopping, visiting social networks, blogging, etc.) that exposes them to malware much more frequently than a device used strictly for business purposes. That malware may then be spread throughout the company. In addition, many users do not password protect their laptops, tablets, and smartphones or set the timeout to automatically lock the device after a few minutes of not being used. All these create an environment ripe for potential security problems.

It is worth noting that employees also have concerns with BYOD policies, primarily related to privacy. Most people place a high priority on keeping any prying eyes, including those of their employer, from looking at the personal photos, text messages, and email stored on their personal mobile devices.

Growing Reliance on Commercial Software with Known Vulnerabilities

In computing, an **exploit** is an attack on an information system that takes advantage of a particular system vulnerability. Often this attack is due to poor system design or implementation. Once the vulnerability is discovered, software developers create and issue a “fix,” or patch, to eliminate the problem. Users of the system or application are responsible for obtaining and installing the patch, which they can usually download from the web.

Any delay in installing a patch exposes the user to a potential security breach. The need to install a fix to prevent a hacker from taking advantage of a known system vulnerability can create a time-management dilemma for system support personnel trying to balance a busy work schedule. Should they install a patch that, if left uninstalled, could lead to a security breach, or should they complete assigned project work so that the anticipated project savings and benefits from the project can begin to accrue on schedule? According to the National Vulnerability Database (the U.S. government repository of standards-based vulnerability management data), the number of new software vulnerabilities identified in 2015 dropped 18 percent from the previous year to 6,480, as shown in Figure 3-1.[10]

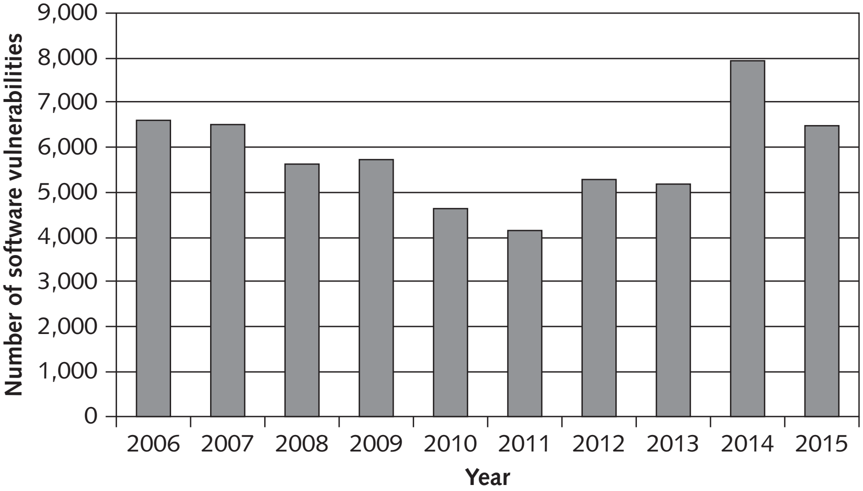


FIGURE 3-1 Total number of software vulnerabilities

Source: National Vulnerability Database

Clearly, it can be difficult to keep up with all the required patches to fix these vulnerabilities, and U.S. companies increasingly rely on commercial software with known vulnerabilities. Even when vulnerabilities are exposed, many corporate IT organizations prefer to use already installed software as is rather than implement security fixes that will either make the software harder to use or eliminate "nice-to-have" features that will help sell the software to end users.

Increasing Sophistication of Those Who Would Do Harm

Previously, the stereotype of a computer troublemaker was that of an introverted "geek" working on his or her own and motivated by the desire to gain some degree of notoriety. This individual was armed with specialized, but limited, knowledge of computers and networks and used rudimentary tools, perhaps downloaded from the Internet, to execute his or her exploits. While such individuals still exist, it is not this stereotyped individual who is the biggest threat to IT security. Today's computer menace is much better organized and may be part of an organized group (for example, Anonymous, Chaos Computer Club, Lizard Squad, TeslaTeam, and hacker teams sponsored by national governments) that has an agenda and targets specific organizations and websites. Some of these groups have ample resources, including money and sophisticated tools to support their efforts. Today's computer attacker has greater depth of knowledge and expertise in getting around computer and network security safeguards. Table 3-1 summarizes the types of perpetrators of computer mischief, crime, and damage.

TABLE 3-1 Classifying perpetrators of computer crime

Type of perpetrator	Description
Black hat hacker	Someone who violates computer or Internet security maliciously or for illegal personal gain (in contrast to a white hat hacker who is someone who has been hired by an organization to test the security of its information systems)
Cracker	An individual who causes problems, steals data, and corrupts systems
Malicious insider	An employee or contractor who attempts to gain financially and/or disrupt a company's information systems and business operations
Industrial spy	An individual who captures trade secrets and attempts to gain an unfair competitive advantage
Cybercriminal	Someone who attacks a computer system or network for financial gain
Hacktivist	An individual who hacks computers or websites in an attempt to promote a political ideology
Cyberterrorist	Someone who attempts to destroy the infrastructure components of governments, financial institutions, and other corporations, utilities, and emergency response units

Types of Exploits

There are numerous types of computer attacks, with new varieties being invented all the time. This section discusses some of the more common attacks, including ransomware, viruses, worms, Trojan horses, blended threats, spam, distributed denial-of-service (DDoS) attacks, rootkits, advanced persistent threats, phishing and spear phishing, smishing and vishing, cyberespionage, and cyberterrorism.

While we usually think of such exploits being aimed at computers, smartphones continue to become more computer capable. Increasingly, smartphone users store an array of personal identity information on their devices, including credit card numbers and bank account numbers. Smartphones are used to surf the web and transact business electronically. The more people use their smartphones for these purposes, the more attractive these devices become as targets for cyberthieves. One form of smartphone malware runs up charges on users' accounts by automatically sending messages to numbers that charge fees upon receipt of a message.

Ransomware

Ransomware is malware that stops you from using your computer or accessing your data until you meet certain demands, such as paying a ransom or sending photos to the attacker. A computer becomes infected with ransomware when a user opens an email attachment containing the malware or is lured to a compromised website by a deceptive email or pop-up window. Ransomware can also be spread through removable USB drives or by texting applications such as Yahoo Messenger, with the payload disguised as an image.

In early February 2016, Hollywood Presbyterian Medical Center was forced to shut down its computer network after hackers encrypted some of its data and demanded a ransom be paid before the data would be unlocked. Initially, the hospital refused to pay the ransom, and hospital employees were forced to resort to paper, pencil, phones, and fax machines to carry out many of their tasks, including accessing patient data. The hospital sought help from the FBI, the Los Angeles Police Department, and cybersecurity consultants, but it was unable to access the data. After a week, the hospital paid the ransom of $12,000. By February 15, access to the data was fully restored, and according to a hospital spokesperson, there was no evidence that any patient or employee data had been accessed.[11]

Viruses

Computer virus has become an umbrella term for many types of malicious code. Technically, a **virus** is a piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner. For example, a virus may be programmed to display a certain message on an infected computer's display screen, delete or modify a certain document, or reformat the hard drive. Almost all viruses are attached to a file, meaning the virus executes only when the infected file is opened. A virus is spread to other machines when a computer user shares an infected file or sends an email with a virus-infected attachment. In other words, viruses are spread by the action of the "infected" computer user.

Macro viruses have become a common and easily created form of virus. Attackers use an application macro language (such as Visual Basic or VBScript) to create programs that infect documents and templates. After an infected document is opened, the virus is executed and infects the user's application templates. Macros can insert unwanted words, numbers, or phrases into documents or alter command functions. After a macro virus infects a user's application, it can embed itself in all future documents created with the application. The "WM97/Resume.A" virus is a Word macro virus spread via an email message with the subject line “Resume - Janet Simons.” If the email recipient clicks on the attachment, the virus deletes all data in the user’s computer or mobile device.

Worms

Unlike a computer virus, which requires users to spread infected files to other users, a **worm** is a harmful program that resides in the active memory of the computer and duplicates itself. Worms differ from viruses in that they can propagate without human intervention, often sending copies of themselves to other computers by email. A worm is capable of replicating itself on your computer so that it can potentially send out thousands of copies of itself to everyone in your email address book, for example.

The negative impact of a worm attack on an organization’s computers can be considerable—lost data and programs, lost productivity due to workers being unable to use their computers, additional lost productivity as workers attempt to recover data and programs, and lots of effort for IT workers to clean up the mess and restore everything to as close to normal as possible. The cost to repair the damage done by each of the Code Red, SirCam, and Melissa worms was estimated to exceed $1 billion, with that of the Conficker, Storm, and ILOVEYOU worms totaling well over $5 billion.[12,13]

Trojan Horses

A **Trojan horse** is a seemingly harmless program in which malicious code is hidden. A victim on the receiving end of a Trojan horse is usually tricked into opening it because it appears to be useful software from a legitimate source, such as an update for software the user currently has installed on his or her computer. The program’s harmful payload might be designed to enable the hacker to destroy hard drives, corrupt files, control the computer remotely, launch attacks against other computers, steal passwords, or spy on users by recording keystrokes and transmitting them to a server operated by a third party. A Trojan horse often creates a “backdoor” on a computer that enables an attacker to gain future access to the system and compromise confidential or private information.

A Trojan horse can be delivered via an email attachment, downloaded to a user’s computer when he or she visits a website, or contracted via a removable media device, such as a DVD or USB memory stick. Once an unsuspecting user executes the program that hosts the Trojan horse, the malicious payload is automatically launched as well—with no telltale signs. Common host programs include screen savers, greeting card systems, and games.

Department of Homeland Security (DHS) officials say they have evidence that harmful Trojan horse malware has been planted in the software that runs much of the U.S. critical infrastructure, including oil and gas pipelines, power transmission grids, water distribution and filtration systems, and even nuclear power generation plants. DHS believes that the malware was planted by the Russians as early as 2011 as a deterrent to a U.S. cyberattack on Russia. The Trojan horse would allow nonauthorized users to control or shut down key components of U.S. infrastructure remotely from their computer or mobile device.[14]

Another type of Trojan horse is a **logic bomb**, which executes when it is triggered by a specific event. For example, logic bombs can be triggered by a change in a particular file, by typing a specific series of keystrokes, or at a specific time or date. Malware attacks employing logic bombs compromised some 32,000 Windows, Unix, and Linux systems at half a dozen South Korean organizations, including three major television broadcasters and two large banks. A component of the attack was "wiper" malware triggered by a logic bomb set to begin overwriting a computer's master boot record at a preset time and day.[15]

Blended Threat

A **blended threat** is a sophisticated threat that combines the features of a virus, worm, Trojan horse, and other malicious code into a single payload. A blended threat attack might use server and Internet vulnerabilities to initiate and then transmit and spread an attack on an organization's computing devices, using multiple modes to transport itself, including email, Internet Relay Chat (IRC), and file-sharing networks. Rather than launching a narrowly focused attack on specific EXE files, a blended threat might attack multiple EXE files, HTML files, and registry keys simultaneously.

Spam

Email **spam** is the use of email systems to send unsolicited email to large numbers of people. Most spam is a form of low-cost commercial advertising, sometimes for questionable products such as pornography, phony get-rich-quick schemes, and worthless stock. Spam is also an extremely inexpensive marketing tool used by many legitimate organizations. For example, a company might send email to a broad cross section of potential customers to announce the release of a new product in an attempt to increase initial sales. However, spam is also used to deliver harmful worms and other malware.

The cost of creating an email campaign for a product or service can be several hundreds to a few thousand dollars, compared to tens of thousands of dollars for direct-mail campaigns. In addition, email campaigns might take only a couple of weeks (or less) to develop, compared with three months or more for direct-mail campaigns, and the turnaround time for feedback averages 48 hours for email as opposed to weeks for direct mail. However, the benefits of spam to companies may be largely offset by the public's generally negative reaction to receiving unsolicited ads.

Spam forces unwanted and often objectionable material into email boxes, detracts from the ability of recipients to communicate effectively due to full mailboxes and relevant emails being hidden among many unsolicited messages, and costs Internet users and service providers millions of dollars annually. It takes user's time to scan and delete spam email, a cost that can add up if they pay for Internet connection charges on an hourly basis (such as at an Internet café). It also costs money for Internet service providers (ISPs) and online services to transmit spam, which is reflected in the rates charged to all subscribers.

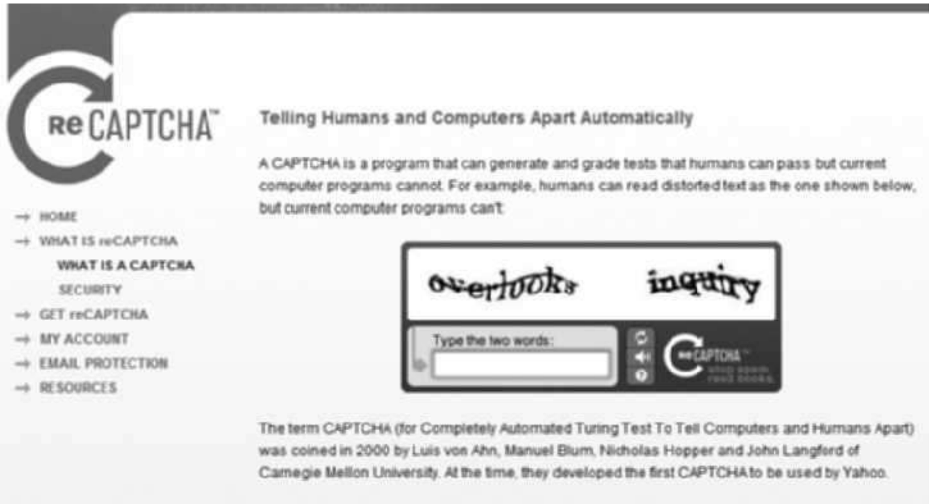
There is an even more sinister side to spam—often it is used to entice unsuspecting recipients to take actions that will result in malware being downloaded to their computer. In early 2015, Symantec, a provider of security, storage, and systems management solutions, began noticing multiple instances of short-duration, high-volume spam attacks targeting millions of users. The messages instructed recipients to click on a link to a URL, which, if done, resulted in the Trojan "Infostealer.Dyranges

(Dyre)" being downloaded to their computer. This Trojan is known to steal financial information.[16]

The **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act** states that it is legal to spam, provided the messages meet a few basic requirements—spammers cannot disguise their identity by using a false return address, the email must include a label specifying that it is an ad or a solicitation, and the email must include a way for recipients to indicate that they do not want future mass mailings. Despite CAN-SPAM and other measures, the percentage of spam in email messages averaged 57 percent in one week in January, 2015, according to Trustwave, an organization that helps businesses protect data and reduce security risk.[17]

Many companies—including Google, Microsoft, and Yahoo!—offer free email services. Spammers often seek to use email accounts from such major, free, and reputable web-based email service providers, as their spam can be sent at no charge and is less likely to be blocked. Spammers can defeat the registration process of the free email services by launching a coordinated bot attack that can sign up for thousands of email accounts. These accounts are then used by the spammers to send thousands of untraceable email messages for free.

A partial solution to this problem is the use of CAPTCHA to ensure that only humans obtain free accounts. **CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart)** software generates and grades tests that humans can pass and all but the most sophisticated computer programs cannot. For example, humans can read the distorted text in Figure 3-2, but simple computer programs cannot.



Telling Humans and Computers Apart Automatically

A CAPTCHA is a program that can generate and grade tests that humans can pass but current computer programs cannot. For example, humans can read distorted text as the one shown below, but current computer programs can't.

Type the two words:

The term CAPTCHA (for Completely Automated Turing Test To Tell Computers and Humans Apart) was coined in 2000 by Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford of Carnegie Mellon University. At the time, they developed the first CAPTCHA to be used by Yahoo.

FIGURE 3-2 Example of CAPTCHA

Source: Courtesy of Carnegie Mellon University

DDoS Attacks

A **distributed denial-of-service (DDoS) attack** is one in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks. A DDoS attack does not involve infiltration of the targeted system. Instead, it keeps the target so busy responding to a stream of automated requests that legitimate users cannot get in—the Internet equivalent of dialing a telephone number repeatedly so that all other callers hear a busy signal. The targeted machine essentially holds the line open while waiting for a reply that never comes; eventually, the requests exhaust all resources of the target.

The software required to initiate a DDoS is simple to use, and many DDoS tools are readily available at a variety of hacker sites. In a DDoS attack, a tiny program is downloaded surreptitiously from the attacker's computer to dozens, hundreds, or even thousands of computers all over the world. The term **botnet** is used to describe a large group of such computers, which are controlled from one or more remote locations by hackers, without the knowledge or consent of their owners. The collective processing capacity of some botnets exceeds that of the world's most powerful supercomputers. Based on a command by the attacker or at a preset time, the botnet computers (called **zombies**) go into action, each sending a simple request for access to the target site again and again—dozens of times per second. The target computers become so overwhelmed by requests for service that legitimate users are unable to get through to the target computer.

Dyn is an Internet performance management company that provides network services including Domain Name System (DNS) services for its many clients. DNS is a large distributed database that translates the domain name you enter into your browser (for example, soccervillage.com) into the IP address of the device hosting the website for that domain name (for example, 206.35.184.101). Without DNS, your website is "invisible" to users who only know it by its domain name. Starting October 21, 2016, Dyn was hit with a series of massive DDoS attacks. Millions of users on the East coast were unable to reach the websites of Dyn's clients, including Airbnb, Amazon, Comcast, Etsy, GoFundMe, New York Times, PayPal, Shopify, and Twitter. The attack had a severe impact on the website owners, who were unable to provide customer services or generate e-commerce revenue.[18]

Rootkit

A **rootkit** is a set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge. Once installed, the attacker can gain full control of the system and even obscure the presence of the rootkit from legitimate system administrators. Attackers can use the rootkit to execute files, access logs, monitor user activity, and change the computer's configuration. Rootkits are one part of a type of blended threat that consists of a dropper, a loader, and a rootkit. The dropper code gets the rootkit installation started and can be activated by clicking on a link to a malicious website in an email or opening an infected PDF file. The dropper launches the loader program and then deletes itself. The loader loads the rootkit into memory; at that point, the computer has been compromised. Rootkits are designed so cleverly that it is difficult even to discover if they are installed on a computer. The fundamental problem with trying to detect a rootkit is that the operating system cannot be trusted to provide valid test results. The following are some symptoms of rootkit infections:

- The computer locks up or fails to respond to input from the keyboard or mouse.
- The screen saver changes without any action on the part of the user.

- The taskbar disappears.
- Network activities function extremely slowly.

When it is determined that a computer has been infected with a rootkit, there is little to do but reformat the disk; reinstall the operating system and all applications; and reconfigure the user's settings, such as mapped drives. This can take hours, and the user may be left with a basic working machine, but all locally held data and settings may be lost.

The "2012 rootkit virus" is a nasty piece of malware that deletes information from a computer and makes it impossible to run some applications, such as Microsoft Word. The longer the rootkit is present, the more damage it causes. The virus asks users to install what appears to be a legitimate update to their antivirus software or some other application. By the time the user sees the prompt to install the software, it is too late; the computer has already been infected by the rootkit.[19]

Advanced Persistent Threat

An **advanced persistent threat (APT)** is a network attack in which an intruder gains access to a network and stays there—undetected—with the intention of stealing data over a long period of time (weeks or even months). Attackers in an APT must continuously rewrite code and employ sophisticated evasion techniques to avoid discovery. APT attacks target organizations with high-value information, such as banks and financial institutions, government agencies, and insurance companies with the goal of stealing data rather than disrupting services.[20] An APT attack advances through the following five phases:

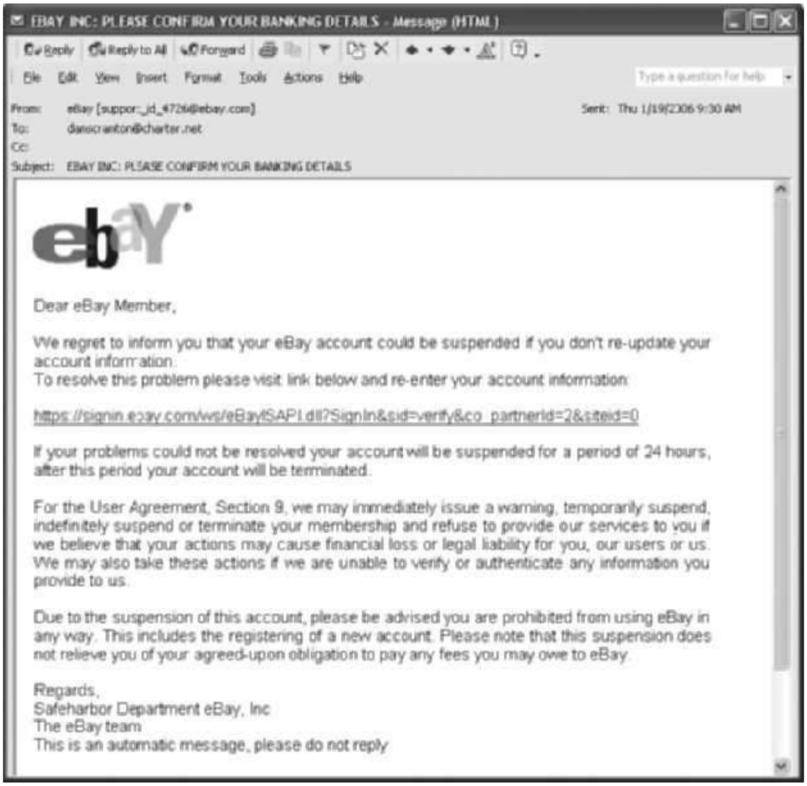
1. Reconnaissance—The intruder begins by conducting reconnaissance on the network to gain useful information about the target (security software installed, computing resources connected to the network, number of users).
2. Incursion—The attacker next launches incursions to gain access to the network at a low level to avoid setting off any alarms or suspicion. Some forms of spear phishing may be employed in this phase. After gaining entrance, the attacker establishes a back door, or a means of accessing a computer program that bypasses security mechanisms.
3. Discovery—The intruder now begins a discovery process to gather valid user credentials (especially administrative ones) and move laterally across the network, installing more back doors. These back doors enable the attacker to install bogus utilities for distributing malware that remains hidden in plain sight.
4. Capture—The attacker is now ready to access unprotected or compromised systems and capture information over a long period of time.
5. Export—Captured data are then exported back to the attacker's home base for analysis and/or used to commit fraud and other crimes.[21]

Although APT attacks are difficult to identify, the theft of data can never be completely invisible. Detecting anomalies in outbound data is perhaps the best way for an administrator to discover that the network has been the target of an APT attack.

The hacker group Carbanak is thought to have stolen over $1 billion from banks in China, Russia, the Ukraine, and the United States. The group's modus operandi include use of an APT that initially hooks its victims using spear phishing emails imitating legitimate banking communications. The group performs a reconnaissance phase to gather data about system administrators and then uses this information to navigate through various bank systems, including ATMs, financial accounts, and money processing services. Once access to these systems is gained, the hackers steal money by transferring funds to accounts in China and the United States. They have even programmed ATMs to dispense money at specific times for collection by money mules.[22]

Phishing

Phishing is the act of fraudulently using email to try to get the recipient to reveal personal data. In a phishing scam, con artists send legitimate-looking emails urging the recipient to take action to avoid a negative consequence or to receive a reward. The requested action may involve clicking on a link to a website or opening an email attachment. These emails, such as the one shown in Figure 3-3, lead consumers to counterfeit websites designed to trick them into divulging personal data or to download malware onto their computers.



From: eBay [suppor_id_4726@ebay.com]
Sent: Thu 1/19/2006 9:30 AM
To: danscranton@charter.net
Cc:
Subject: EBAY INC: PLEASE CONFIRM YOUR BANKING DETAILS

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

FIGURE 3-3 Example of a phishing email

The volume of global phishing attacks is alarming. It is estimated that about 156 million phishing emails are sent each day, with 16 million of those successfully evading email filters. Of those, roughly 50 percent (or 8 million) are opened, and 800,000 recipients per day click on malicious URL links contained in the emails.[23]

Savvy users often become suspicious and refuse to enter data into the fake websites; however, sometimes just accessing the website can trigger an automatic and unnoticeable download of malicious software to a computer. Indeed, the percentage of malicious URLs in unsolicited emails surged to an average of 10 percent in 2014.[24] As one might guess, financial institutions such as Bank of America, Citibank, Chase, MasterCard, Visa, and Wells Fargo are among the websites that phishers spoof most frequently.

Spear phishing is a variation of phishing in which the phisher sends fraudulent emails to a certain organization's employees. It is known as spear phishing because the attack is much more precise and narrow, like the tip of a spear. The phony emails are designed to look like they came from high-level executives within the organization. Employees are directed to a fake website and then asked to enter personal information, such as name, Social Security number, and network passwords. Botnets have become the primary means for distributing phishing scams.

In early 2016, more than three dozen large and small organizations were victimized by spear phishing attacks that were designed to obtain data from employee tax records. Many of these attacks spoofed the email address of the CEO, CFO, or someone else of authority within the organization, prompting many employees to comply with the request.[25]

Smishing and Vishing

Smishing is another variation of phishing that involves the use of texting. In a smishing scam, people receive a legitimate-looking text message telling them to call a specific phone number or log on to a website. This is often done under the guise that there is a problem with the recipient's bank account or credit card that requires immediate attention. However, the phone number or website is phony and is used to trick unsuspecting victims into providing personal information such as a bank account number, personal identification number, or credit card number, which can then be used to steal money from victims' bank accounts, charge purchases on their credit cards, or open new accounts. In some cases, if victims log on to a website, malicious software is downloaded onto their smartphones, providing criminals with access to information stored on the phones. The number of smishing scams typically increases around the holidays as more people use their smartphones to make online purchases.

Vishing is similar to smishing except that the victims receive a voice-mail message telling them to call a phone number or access a website. One recent vishing campaign captured the payment card information of an estimated 250 Americans per day. In the attack, users were sent a message that their ATM card had been deactivated. The users were prompted to call a phone number to reactivate the card by entering their card number and their personal identification number (PIN)—data that were recorded and then used by the criminals to withdraw money from the accounts.[26]

Financial institutions, credit card companies, and other organizations whose customers may be targeted by criminals in this manner should be on the alert for phishing, smishing, and vishing scams. They must be prepared to act quickly and decisively, without alarming their customers if such a scam is detected. Recommended action steps for institutions and organizations include the following:

- Companies should educate their customers about the dangers of phishing, smishing, and vishing through letters, recorded messages for those calling into the company's call center, and articles on the company's website.
- Call center service employees should be trained to detect customer complaints that indicate a scam is being perpetrated. They should attempt to capture key pieces of information, such as the callback number the customer was directed to use, details of the phone message or text message, and the type of information requested.
- Customers should be notified immediately if a scam occurs. This can be done via a recorded message for customers phoning the call center, working with local media to place a news article in papers serving the area of the attack, placing a banner on the institution's web page, and even displaying posters in bank drive-through and lobby areas.
- If it is determined that the calls are originating from within the United States, companies should report the scam to the FBI.
- Institutions can also try to notify the telecommunications carrier for the particular numbers to request that they shut down the phone number's victims are requested to call.[27]

Cyberespionage

Cyberespionage involves the deployment of malware that secretly steals data in the computer systems of organizations, such as government agencies, military contractors, political organizations, and manufacturing firms. The type of data most frequently targeted includes data that can provide an unfair competitive advantage to the perpetrator. These data are typically not public knowledge and may even be protected via patent, copyright, or trade secret. High-value data include the following:

- Sales, marketing, and new product development plans, schedules, and budgets
- Details about product designs and innovative processes
- Employee personal information
- Customer and client data
- Sensitive information about partners and partner agreements

Tensions have long simmered between the China and the United States over alleged cyberattacks. The U.S. experts claim cyberespionage has helped China to accelerate the research and development process and cut years off the time for that country to acquire new technology in a variety of industries. Alleged targets have included aluminum and steel producers, a company that designs nuclear power plants, a solar panel manufacturer, and an aircraft manufacturer. Meanwhile, China's Foreign Ministry portrays the United States as a hypocrite that engages in cyberespionage by conducting cybertheft, wiretapping, and surveillance activities against Chinese governmental departments, companies, and universities. After years of discussion and behind-the-scenes efforts, President Obama and Chinese President Xi announced in 2015 that the two nations had agreed to initial norms of cyberactivities with the two nations pledging each will avoid conducting cybertheft of intellectual property for commercial gain.[28,29] United States and Chinese officials met again in May 2016 to discuss cybersecurity issues. While no details of the meeting were revealed, the United States State Department stated that "international norms of state behavior and other crucial issues for international security in cyberspace" were addressed. While a statement from China's foreign ministry reported that there was a "positive, deep and constructive discussion" between the two countries, it remains to be seen how much of an impact this agreement will have.[30]

Cyberterrorism

Cyberterrorism is the intimidation of government or civilian population by using information technology to disable critical national infrastructure (for example, energy, transportation, financial, law enforcement, and emergency response) to achieve political, religious, or ideological goals. It is an increasing concern for countries and organizations around the globe. Indeed, in a statement released by the White House in early 2015, President Obama said, "Cyber threats pose one of the gravest national security dangers that the United States faces."[31]

The **Department of Homeland Security (DHS)** is a large federal agency with more than 240,000 employees and a budget of almost $65 billion whose goal is to provide for a "safer, more secure America, which is resilient against terrorism and other potential threats." The agency was formed in 2002 when 22 different federal departments and agencies were combined into a unified, integrated cabinet agency.[32] The agency's Office of Cybersecurity and Communications resides within the National Protection and Programs Directorate and is responsible for enhancing the security, resilience, and reliability of U.S. cyber and communications infrastructure. It works to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services.[33] The DHS website (*www.dhs.gov*) provides a link that enables users to report cyber incidents. Incident reports go to the US-CERT Incident Reporting System, which assists analysts at the **U.S. Computer Emergency Readiness Team (US-CERT)** (a partnership between the DHS and the public and private sectors) in providing timely handling of security incidents as well as in conducting improved analysis of such incidents.[34] Established in 2003 to protect the nation's Internet infrastructure against cyberattacks, US-CERT serves as a clearinghouse for information on new viruses, worms, and other computer security topics.

Cyberterrorists try on a daily basis to gain unauthorized access to a number of important and sensitive sites, such as the computers at the British, French, Israeli, and U.S. foreign intelligence agencies; North American Aerospace Defense Command (NORAD); and numerous government ministries and private companies around the world.

In late 2015, cyberterrorists attacked the two electric utility companies in western Ukraine, causing a three-hour power outage affecting some 80,000 customers. Not only did the hackers cut the power, they also froze the data displayed on the screens of plant operators so they could not view the changing plant conditions; thus, fooling the operators into believing power was still flowing. To prolong the outage, the attackers also launched a telephone DDoS attack against the utility's call center to prevent customers from reporting the outage—the center's phone system was flooded with bogus calls to prevent legitimate callers from getting through. Once operators became aware of the outage, the attackers activated KillDisk malware that rendered infected servers and systems unusable. The operators' machines were completely destroyed by the malware.[35]

Federal Laws for Prosecuting Computer Attacks

Over the years, several laws have been enacted to help prosecute those responsible for computer-related crimes; these are summarized in Table 3-2. For example, Section 814 of the USA Patriot Act defines cyberterrorism as any hacking attempts designed to gain unauthorized access to a protected computer, which, if successful, would cause a person an aggregate loss greater than $5,000; adversely affect someone's medical examination, diagnosis, or treatment; cause a person to be injured; cause a threat to public health or safety; or cause damage to a governmental computer that is used as a tool to administer justice, national defense, or national security.[36] Those convicted of cyberterrorism are subject to a prison term of 5 to 20 years. (The $5,000 threshold is quite easy to exceed, and, as a result, many young people who have been involved in what they consider to be minor computer pranks have found themselves meeting the criteria to be tried as cyberterrorists.)

TABLE 3-2 Federal laws that address computer crime

Federal law	Subject area
Computer Fraud and Abuse Act (U.S. Code Title 18, Section 1030)	Addresses fraud and related activities in association with computers, including the following: • Accessing a computer without authorization or exceeding authorized access • Transmitting a program, code, or command that causes harm to a computer • Trafficking of computer passwords • Threatening to cause damage to a protected computer
Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029)	Covers false claims regarding unauthorized use of credit cards
Stored Wire and Electronic Communications and Transactional Records Access Statutes (U.S. Code Title 18, Chapter 121)	Focuses on unlawful access to stored communications to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage
USA Patriot Act (Public Law 107-56)	Defines cyberterrorism and associated penalties

CRITICAL THINKING EXERCISE: HIRING A BLACK HAT HACKER

You are a member of the human resources department of a software manufacturer that has several products and annual revenue in excess of $500 million. You're on the phone with the manager of software development who has made a request to hire a notorious black hat hacker to probe your company's software products in an attempt to identify any vulnerabilities. The reasoning is that if anyone can find a vulnerability in your software, she can. This will give your firm a head start on developing patches to fix the problems before anyone can exploit them. You feel uneasy about hiring people with criminal records and connections to unsavory members of the hacker/cracker community and are unsure if you should approve the hire. Provide three good reasons to hire this individual. Provide three good reasons not to hire this individual. How would you respond to this request? Why?

Now that we have discussed various types of computer exploits, the people who perpetrate these exploits, and the laws under which they can be prosecuted, we will discuss how organizations can take steps to implement a trustworthy computing environment to defend against such attacks.

THE CIA SECURITY TRIAD

The IT security practices of organizations worldwide are focused on ensuring confidentiality, maintaining integrity, and guaranteeing the availability of systems and data. Confidentiality ensures that only those individuals with the proper authority can access sensitive data such as employee personal data, customer and product sales data, and new product and advertising plans. Integrity ensures that data can only be changed by authorized individuals so that the accuracy, consistency, and trustworthiness of data are guaranteed. Availability ensures that the data can be accessed when and where needed, including during times of both normal and disaster recovery operations. A widely held but difficult-to-achieve standard of availability for a system or product is known as "five 9s" or 99.999 percent availability. For an operation that runs 365 days per year, 24 hours per day this translates to less than one hour of unavailability per year. Confidentiality, integrity, and availability are referred to as the **CIA security triad**.

No organization can ever be completely secured from an attack. The key to prevention of a computer security incident is to implement a layered security solution to make computer break-ins so difficult that an attacker eventually gives up or is detected before much harm is inflicted. In a layered solution, if an attacker breaks through one layer of security, another layer must then be overcome. Security measures must be planned for, designed, implemented, tested, and maintained at the organization, network, application, and end-user levels to achieve true CIA security (see Figure 3-4). These layers of protective measures are explained in more detail in the following sections.

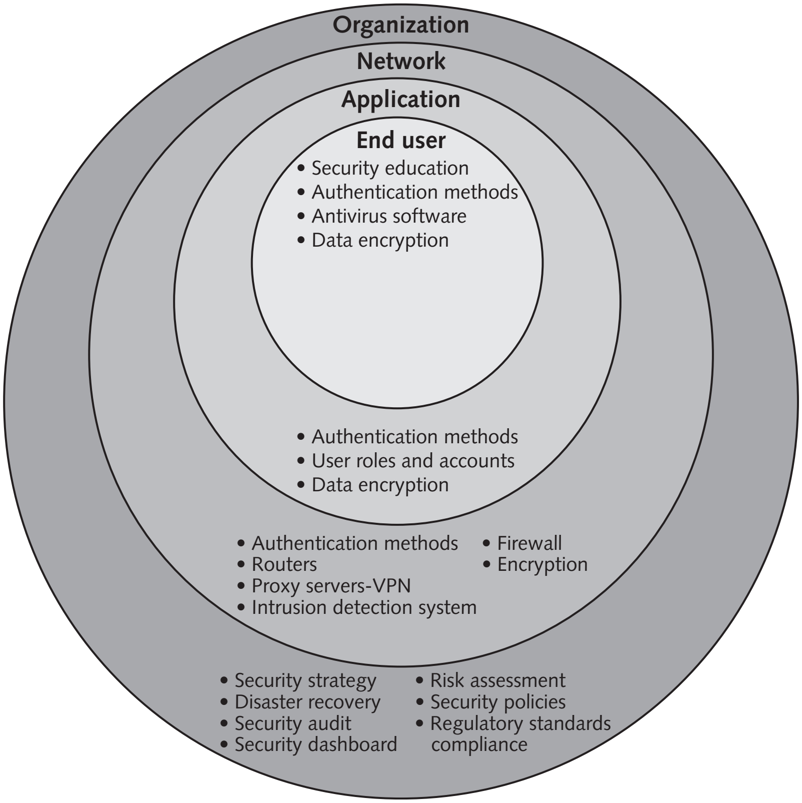


FIGURE 3-4 Implementing CIA security at the organization, network, application, and end-user levels

Implementing CIA at the Organization Level

Implementing CIA begins at the organization level with the definition of an overall security strategy, performance of a risk assessment, laying out plans for disaster recovery, setting security policies, conducting security audits, ensuring regulatory standards compliance, and creating a security dashboard. Completion of these tasks at the organizational level will set a sound foundation and clear direction for future CIA-related actions.

Security Strategy

Implementing CIA security at the organization level requires a risk-based security strategy with an active governance process to minimize the potential impact of any security incident and to ensure business continuity in the event of a cyberattack. Creating such a strategy typically begins with performing a risk assessment to identify and prioritize the threats that the organization faces. The security strategy must define a disaster recovery plan that ensures the availability of key data and information technology assets. Security policies are needed to guide employees to follow recommended processes and practices to avoid security-related problems. Periodic security audits are needed to ensure that individuals are following established policies and to assess if the policies are still adequate even under changing conditions. In addition to complying with its internal policies, an organization may also need to comply with standards defined by external parties, including regulatory agencies. Many organizations employ a security dashboard to help track the key performance indicators of their security strategy. The various components of the security strategy will now be defined.

Risk Assessment

Risk assessment is the process of assessing security-related risks to an organization's computers and networks from both internal and external threats. Such threats can prevent an organization from meeting its key business objectives. The goal of risk assessment is to identify which investments of time and resources will best protect the organization from its most likely and serious threats. In the context of an IT risk assessment, an asset is any hardware, software, information system, network, or database that is used by the organization to achieve its business objectives. A loss event is any occurrence that has a negative impact on an asset, such as a computer contracting a virus or a website undergoing a DDoS attack. The steps in a general security risk assessment process are as follows:

- Step 1—Identify the set of IT assets about which the organization is most concerned. Priority is typically given to those assets that support the organization's mission and the meeting of its primary business goals.
- Step 2—Identify the loss events or the risks or threats that could occur, such as a DDoS attack or insider fraud.
- Step 3—Assess the frequency of events or the likelihood of each potential threat; some threats, such as insider fraud, are more likely to occur than others.
- Step 4—Determine the impact of each threat occurring. Would the threat have a minor impact on the organization, or could it keep the organization from carrying out its mission for a lengthy period of time?
- Step 5—Determine how each threat can be mitigated so that it becomes much less likely to occur or, if it does occur, has less of an impact on the organization. Due to time and resource limitations, most organizations choose to focus on just those threats that have a high (relative to all other threats) probability of occurrence and a high (relative to all other threats) impact. In other words, first address those threats that are likely to occur and that would have a high negative impact on the organization.
- Step 6—Assess the feasibility of implementing the mitigation options.
- Step 7—Perform a cost-benefit analysis to ensure that your efforts will be cost-effective. No amount of resources can guarantee a perfect security system, so organizations must balance the risk of a security breach with the cost of preventing one. The concept of **reasonable assurance** in connection with IT security recognizes that managers must use their judgment to ensure that the cost of control does not exceed the system's benefits or the risks involved.
- Step 8—Make the decision on whether or not to implement a particular countermeasure. If you decide against implementing a particular countermeasure, you need to reassess if the threat is truly serious and, if so, identify a less costly countermeasure.

The general security risk assessment process—and the results of that process—will vary by organization. Table 3-3 illustrates a risk assessment for a hypothetical organization.

TABLE 3-3 Risk assessment for a hypothetical company

Adverse event	Business objective threatened	Threat (estimated frequency of event) per year	Vulnerability (likelihood of success of this threat) (%)	Estimated cost of a successful attack ($)	Risk = Threat × Vulnerability × Estimated cost ($)	Relative priority to be fixed
Data breach of customer account data	Provide a safe, secure website that consumers can trust	18	3	5,000,000	2,700,000	1
Distributed DDoS attack	24/7 operation of a retail website	3	25	500,000	375,000	2
Email attachment with harmful worm	Rapid and reliable communications among employees and suppliers	1,000	0.05	200,000	100,000	3
Harmful virus	Employees' use of personal productivity software	2,000	0.04	50,000	40,000	4
Invoice and payment fraud	Reliable cash flow	1	10	200,000	20,000	5

A completed risk assessment identifies the most dangerous threats to a company and helps focus security efforts on the areas of highest payoff.

Disaster Recovery

Data availability requires implementing products, services, policies, and procedures that ensure that data are accessible even during disaster recovery operations. To accomplish this goal, organizations typically implement a **disaster recovery plan**, which is a documented process for recovering an organization's business information system assets—including hardware, software, data, networks, and facilities—in the event of a disaster.

A disaster recovery plan focuses on technology recovery and identifies the people or the teams responsible to take action in the event of a disaster, what exactly these people will do when a disaster strikes, and the information system resources required to support critical business processes. Disasters can be natural (for example, earthquake, fire, and flood) or manmade (for example, accident, civil unrest, and terrorism). When developing a disaster recovery plan, organizations should think in terms of not being able to gain access to their normal place of business for an extended period of time, possibly up to several months.

As part of defining a business continuity plan, an organization should conduct a business impact analysis to identify critical business processes and the resources that support them. The recovery time for an information system resource should match the recovery time objective for the most critical business processes that depend on that resource. Some business processes are more pivotal to continued operations and goal attainment than others. These processes are called **mission-critical processes**. Quickly recovering data and operations for these mission-critical processes can make the difference between failure and survival for an organization. If your billing system doesn't work and you can't send out invoices, your company is at the risk of going out of business due to cash flow issues.

Cloud computing has added another dimension to disaster recovery planning. If your organization is hit by a disaster, information systems that are running in the cloud are likely to be operational and accessible by workers from anywhere they can access the Internet. Data stored in the cloud may be insulated from the effects of a disaster if it is stored at the site of the service provider, which could be hundreds of miles from the organization. On the other hand, if the cloud service provider is hit by a disaster, it may cause a serious business disruption for your organization even if it is otherwise unaffected by a distant disaster. Thus, part of the evaluation of a cloud service provider must include analysis of the provider's disaster recovery plans.

Files and databases can be protected by making a copy of all files and databases changed during the last few days or the last week, a technique called incremental backup. This approach to backup uses an image log, which is a separate file that contains only changes to applications or data. Whenever an application is run, an image log is created that contains all changes made to all files. If a problem occurs with a database, an old database with the last full backup of the data, along with the image log, can be used to re-create the current database.

Organizations can also hire outside companies to help them perform disaster planning and recovery. EMC, for example, offers data backup in its RecoverPoint product.[37] For individuals and some applications, backup copies of important files can be placed on the Internet. Failover is another approach to backup. When a server, network, or database fails or is no longer functioning, failover automatically switches applications and other programs to a redundant or replicated server, network, or database to prevent an interruption of service. SteelEye's LifeKeeper and Application Continuous Availability by NeverFail are examples of failover software.[38,39] Failover is especially important for applications that must be operational at all times.

It is imperative that a disaster plan be practiced and improvements be made to the plan based on the results of the test. Unfortunately, a recent survey of IT managers revealed that as many as one in eight have either never tested their organization's disaster recovery solution or have no idea exactly when it was last tested.[40] One reasonable approach to testing is to simulate a disaster for a single critical portion (for example, order processing or customer billing) of your business during a time of low business activity. The next disaster plan test should then target a different area of the business.

Security Policies

A **security policy** defines an organization's security requirements, as well as the controls and sanctions needed to meet those requirements. A good security policy delineates responsibilities and the behavior expected of members of the organization. A security policy outlines *what* needs to be done but not *how* to do it. The details of *how* to accomplish the goals of the policy are typically provided in separate documents and procedure guidelines.

The SysAdmin, Audit, Network, Security (SANS) Institute's website (*www.sans.org*) offers a number of security-related policy templates that can help an organization to quickly develop effective security policies. The templates and other security policy information can be found at *www.sans.org/security-resources/policies* and provide guidelines for creating various policies, including acceptable use policy, email policy, password protection policy, remote access policy, and software installation policy.

Experienced IT managers understand that users will often attempt to circumvent security policies or simply ignore them altogether. Because of that, automated system rules should mirror an organization's written policies whenever possible. Automated system rules can often be put into practice using the configuration options in a software program. For example, if a written policy states that passwords must be changed every 30 days, then all systems should be configured to enforce this policy automatically.

System administrators must also be vigilant about changing the default usernames and passwords for specific devices when they are added to an organization's network. Cybercriminals and others looking to access the networks of various organizations can easily find information online regarding the default username and password combinations for many vendors' products.

A growing area of concern for security experts is the use of wireless devices to access corporate email, store confidential data, and run critical applications, such as inventory management and sales force automation. Mobile devices such as smartphones can be susceptible to viruses and worms. However, the primary security threat for mobile devices continues to be loss or theft of the device. Wary companies have begun to include special security requirements for mobile devices as part of their security policies. In some cases, users of laptops and mobile devices must use a virtual private network (VPN) (a method employing encryption to provide secure access to a remote computer over the Internet) to gain access to their corporate network.

Security Audits

Another important prevention tool is a **security audit** that evaluates whether an organization has a well-considered security policy in place and if it is being followed. For example, if a policy says that all users must change their passwords every 30 days, the audit must check how well that policy is being implemented. The audit should also review who has access to particular systems and data and what level of authority each user has. It is not unusual for an audit to reveal that too many people have access to critical data and that many people have capabilities beyond those needed to perform their jobs. One result of a good audit is a list of items that needs to be addressed in order to ensure that the security policy is being met.

A thorough security audit should also test system safeguards to ensure that they are operating as intended. Such tests might include trying the default system passwords that are active when software is first received from the vendor. The goal of such a test is to ensure that all such known passwords have been changed.

Some organizations will also perform a penetration test of their defenses. This entails assigning individuals to try to break through the measures and identify vulnerabilities that still need to be addressed. The individuals used for this test are knowledgeable and are likely to take unique approaches in testing the security measures.

Regulatory Standards Compliance

In addition to the requirement to comply with your own security program, your organization may also be required to comply with one or more standards defined by external parties. In that case, your organization's security program must include a definition of what those standards are and how the organization will comply. Regulatory standards that might affect your organization include those shown in Table 3-4.

TABLE 3-4 Additional standards your organization may be required to meet

Act or standard	Who is affected?	Subject matter
Bank Secrecy Act of 190 (Public Law 91-507)—Amended several times, including by provisions in Title III of the USA PATRIOT Act (see 31 USC § 5311–5330 and Title 31 Code of Federal Regulations Chapter X)	Financial institutions	Requires financial institutions in the United States to assist U.S. government agencies in detecting and preventing money laundering
European Union—United States Privacy Shield	Organizations that do business with companies and/or individuals in the European Union	Provides companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce
Federal Information Security Management Act (44 U.S.C. § 3541, et seq.)	Every federal agency	Requires each federal agency to provide information security for the data and information systems that support the agency's operations and assets, including those provided or managed by another agency, contractor, or other source
Foreign Corrupt Practices Act (15 U.S.C. § 78dd-1, et seq.)	Any person who is a citizen, national, or resident of the United States and engages in foreign corrupt practices; also applies to any act by U.S. businesses, foreign corporation's trading securities in the United States, American nationals, U.S. citizens, and U.S. residents acting in furtherance of a foreign corrupt practice whether or not they are physically present in the United States	Makes certain payments to foreign officials and other foreign persons illegal and requires companies to maintain accurate records
Gramm-Leach-Bliley Act (Public Law 106-102)	Companies that offer financial products or services to individuals, such as loans, insurance, or financial and investment advice	Governs the collection, disclosure, and protection of consumers' nonpublic personal information or personally identifiable information
Health Insurance Portability and Accountability Act (Public Law 104–191)	Healthcare clearinghouses, employer-sponsored health plans, health insurers, and medical service providers	Regulates the use and disclosure of an individual's health information
Payment Card Industry Data Security Standard (PCI DSS)	All organizations that store, process, and transmit cardholder data, most notably for debit cards and credit cards	Provides a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information
Sarbanes-Oxley Act (Public Law 107–204 116 Stat. 745)	All public corporations	Protects shareholders and the general public from accounting errors and fraudulent practices in the enterprise

Security Dashboard

Many organizations use security dashboard software to provide a comprehensive display of all key performance indicators related to an organization's security defenses, including threats, exposures, policy compliance, and incident alerts. The purpose of a security dashboard is to reduce the effort required to monitor and identify threats in time to take action. Data that appear in a security dashboard can come from a variety of sources, including security audits, firewalls, applications, servers, and other hardware and software devices. Figure 3-5 shows an example of a security dashboard.

#	Key performance measure	Goal	Actual	Status
1	Number of segregation-of-duty violations	0	2	Red
2	Number of users with weak, noncompliant passwords	<5	4	Green
3	Percentage of critical IT assets that passed penetration tests	>96%	93%	Yellow
4	Backlog of software security patches and updates	<3	3	Green
5	Number of days since last internal security audit	<90	94	Yellow
6	Percentage of employees and contractors who passed security exam	>95%	87%	Red
7	Score on last disaster-recovery test	>90%	93%	Green

Red - Immediate action required
Yellow -Caution, should be monitored
Green - OK, goal has been met

FIGURE 3-5 Organizational security dashboard

Algoma Central Corporation, a leading Canadian shipping company, owns and operates the largest Canadian flag fleet of dry-bulk carriers and product tankers operating on the Great Lakes—St. Lawrence Seaway system. The firm recently implemented a security dashboard from Avaap, Inc., to improve access to security information and alleviate the complexity of managing security data for its shipping operations.[41]

Implementing CIA at the Network Level

The Internet provides a wide-open and well-travelled pathway for anyone in the world to reach your organization's network. As a result, organizations are continuing to move more of their business processes to the Internet to better serve customers, suppliers, employees, investors, and business partners. However, unauthorized network access by a hacker or resentful employee can result in compromised sensitive data and severely degrade services, with a resulting negative impact on productivity and operational capability. This, in turn, can create a severe strain on relationships with customers, suppliers, employees, investors, and business partners, who may question the capability of the organization to protect its confidential information and offer reliable services. Organizations must carefully manage the security of their networks and implement strong measures to ensure that sensitive data are not accessible to anyone who is not authorized to see it.

Authentication Methods

To maintain a secure network, an organization must authenticate users attempting to access the network by requiring them to enter a username and password; inserting a smart card and entering the associated PIN; or providing a fingerprint, voice pattern sample, or retina scan. The Federal Financial Institutions Examination Council has developed a set of guidelines called "Authentication in an Internet Banking Environment," which recommends a two-factor authorization. This approach adds another identity check along with the password system. A number of multifactor authentication schemes can be used, such as biometrics, one-time passwords, or hardware tokens that plug into a USB port on the computer and generate a password that matches the one used by a bank's security system.[42]

The use of biometric technology has been slow to develop due to cost and privacy concerns. However, MasterCard recently announced it will begin rolling out its new MasterCard Identity Check service that allows users to take an initial ID photo that will be used to create a digital map of their face, which will be stored on MasterCard's servers. When the user wants to make a payment using a smartphone, the MasterCard app will capture his or her image, which, along with a user-entered password, will be authenticated against the stored image before the transaction is approved. MasterCard's system also offers a fingerprint sensor that can be used to verify purchases.[43] Apple's new Apple Pay system makes use of the fingerprint sensors on newer iPhones. Consumers paying with Apple Pay, which is tied to a credit or debit card, just hold their iPhone close to the contactless reader with their finger on the Touch ID button.[44]

Firewall

Installation of a corporate firewall is the most common security precaution taken by businesses. A **firewall** is a system of software, hardware, or a combination of both that stands guard between an organization's internal network and the Internet and limits network access based on the organization's access policy.

Any Internet traffic that is not explicitly permitted into the internal network is denied entry through a firewall. Similarly, most firewalls can be configured so that internal network users can be blocked from gaining access to websites deemed inappropriate for employees, such as those whose content is based on sex and violence. Most firewalls can also be configured to block instant messaging, access to newsgroups, and other Internet activities.

Software vendors Agnitum, Check Point, Comodo, Kaspersky, and Total Defense provide some of the top-rated firewall software used to protect personal computers. Their software provide antivirus, firewall, antispam, parental control, and phishing protection capabilities and sell for $30 to $80 per single user license.

A **next-generation firewall (NGFW)** is a hardware- or software-based network security system that is able to detect and block sophisticated attacks by filtering network traffic dependent on the packet contents. Compared to first- and second-generation firewalls, a NGFW goes deeper to inspect the content of packets and match sequences of bytes for harmful activities, such as known vulnerabilities, exploit attacks, viruses, and malware.

Routers

A router is a networking device that connects multiple networks together and forwards data packets from one network to another. Often, an ISP installs a router in a subscriber's home to connect the ISP's network to the network within the home.

Routers enable you to create a secure network by assigning it a passphrase so that only individuals who have the passphrase can connect to your network. However, a skilled and committed attacker can break the passphrase to gain access to your network. So, as an additional layer of security, the router provides you the capability to specify the unique media access control (MAC) address of each legitimate device connected to the network and restrict access to any other device that attempts to connect to the network. This effectively enables the router to distinguish legitimate traffic from unsolicited traffic and reject uninvited inbound connections. Most routers also have an option to restrict access to specific websites, thus blocking access to websites that are known to infect user devices with malware.

Encryption

Encryption is the process of scrambling messages or data in such a way that only authorized parties can read it. It is used to protect billions of online transactions each day, enabling consumers to order more than $300 billion in merchandise online and banks to route some $40 trillion in financial transactions each year.[45] It enables organizations to share sensitive sales data, promotion plans, new product designs, and project status data among employees, suppliers, contractors, and others with a need to know. Encryption enables physicians and patients to share sensitive healthcare data with labs, hospitals, and other health treatment facilities as well as insurance carriers. To complete such transactions, sensitive data—including names, physical addresses, email addresses, phone numbers, account numbers, health data, financial data, passwords, and PINs—must be sent and received. Great harm could be done and chaos could ensue if these data were to fall into the wrong hands. Encryption is one means of keeping these data secure.

An **encryption key** is a value that is applied (using an algorithm) to a set of unencrypted text (plaintext) to produce encrypted text that appears as a series of seemingly random characters (ciphertext) that is unreadable by those without the encryption key needed to decipher it. There are two types of encryption algorithms: symmetric and asymmetric. Symmetric algorithms use the same key for both encryption and decryption. Asymmetric algorithms use one key for encryption and a different key for decryption. Advanced Encryption Standard (AES) is the most widely used symmetric algorithm and is entrusted to protect classified U.S. government information. Wireless Protected Access 2 (WPA2), which is the most commonly used security protocol for wireless networks today, employs the AES encryption algorithm.

The ability to keep encrypted data secret is not determined by the encryption algorithm, which is widely known, but rather on the encryption key. The encryption key is chosen from one of a large number of possible encryption keys. In general, the longer the key, the stronger the encryption. Thus, an encryption protocol based on a 56-bit key is not as strong as one based on a 128-bit key. Of course, it is essential that the key be kept secret from possible interceptors. A hacker who obtains the key can recover the original message from the encrypted data. Encryption methods rely on the limitations of computing power for their security. If breaking a code requires too much computing power, even the most determined hacker cannot be successful.

Many online shoppers fear the theft of their credit card numbers and banking information. To help prevent this type of theft, the Transport Layer Security (TLS) communications protocol is used to secure sensitive data. **Transport Layer Security (TLS)** is a communications protocol or system of rules that ensures privacy between communicating applications and their users on the Internet. TLS enables a client (such as a web browser) to initiate a temporary, private conversation with a server (such as an online shopping site or bank). Before the client and server start communicating, they perform an automated process called a "handshake" during which they exchange information about who they are and which secret codes and algorithms they will use to encode their messages to each other. Then, for the duration of the conversation, all the data that pass between the client and server is encrypted so that even if somebody does listen in, they won't be able to determine what is being communicated.

Proxy Servers and Virtual Private Networks

A proxy server serves as an intermediary between a web browser and another server on the Internet that makes requests to websites, servers, and services on the Internet for you (see Figure 3-6). When you enter the URL for a website, the request is forwarded to the proxy server, which relays the request to the server where the website is hosted. The homepage of the website is returned to the proxy server, which then passes it on to you. Thus the website sees the proxy server as the actual visitor and not you.

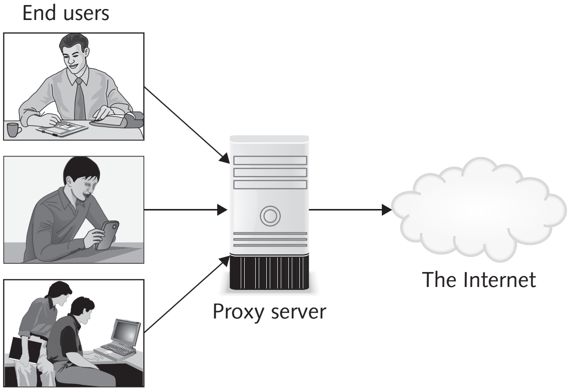


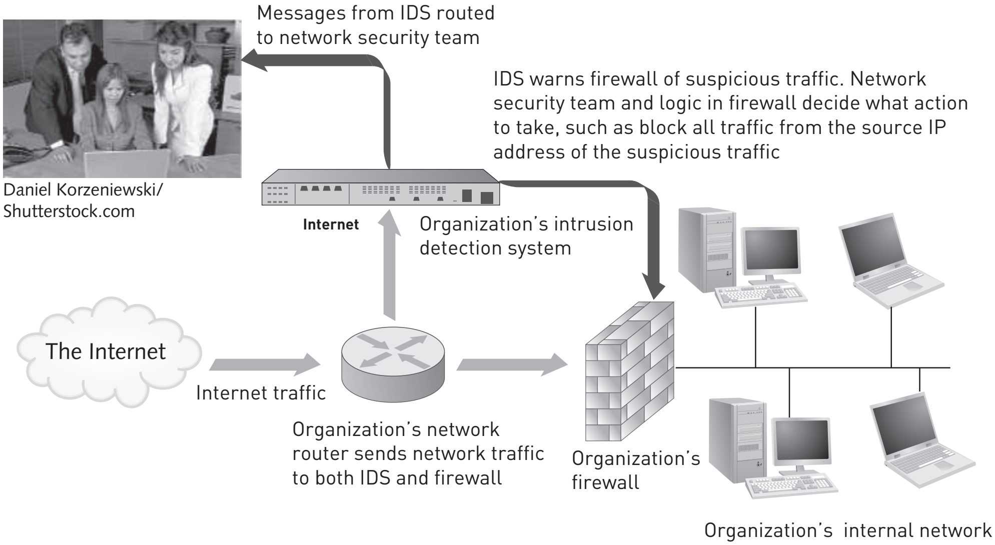
FIGURE 3-6 Proxy server

By forcing employees to access the Internet through a proxy server, companies can prevent employees from accessing certain websites. A proxy server can also capture detailed records of all the websites each employee has visited, when, and for how long. When you access a website directly, the server hosting the website can see your IP address and store cookies on your computer, but a proxy server can hide your IP address and block cookies from being sent to your device. A proxy server relays those packets for you and strips the originating address so instead of your IP address, the website only sees the address of the proxy server.

Remote users working at home, from a client's office, or in a branch office often have a need to access sensitive data on a company's private servers; however, doing so from an unsecured public network, such as a coffee shop wireless hotspot, could expose that data to unauthorized users with ill intentions. A VPN enables remote users to securely access an organization's collection of computing and storage devices and share data remotely. To connect to a VPN, you launch a VPN client on your computer and perform some form of authentication using your credentials. Your computer then exchanges keys to be used for the encryption process with the VPN server. Once both computers have verified each other as authentic, all of your Internet communications are encrypted and secured from eavesdropping.

Intrusion Detection System

An **intrusion detection system (IDS)** is software and/or hardware that monitors system and network resources and activities and notifies network security personnel when it detects network traffic that attempts to circumvent the security measures of a networked computer environment (see Figure 3-7). Such activities usually signal an attempt to breach the integrity of the system or to limit the availability of network resources.


Messages from IDS routed to network security team
IDS warns firewall of suspicious traffic. Network security team and logic in firewall decide what action to take, such as block all traffic from the source IP address of the suspicious traffic
Internet
Organization's intrusion detection system
The Internet
Internet traffic
Organization's network router sends network traffic to both IDS and firewall
Organization's firewall
Organization's internal network

Daniel Korzeniewski/Shutterstock.com

FIGURE 3-7 Intrusion detection system

Knowledge-based approaches and behavior-based approaches are two fundamentally different approaches to intrusion detection. Knowledge-based IDSs contain information about specific attacks and system vulnerabilities and watch for attempts to exploit these vulnerabilities, such as repeated failed login attempts or recurring attempts to download a program to a server. When such an attempt is detected, an alarm is triggered. A behavior-based IDS models normal behavior of a system and its users from reference information collected by various means. The IDS compares current activity to this model and generates an alarm if it finds a deviation. Examples include unusual traffic at odd hours or a user in the human resources department who accesses an accounting program that he or she has never before used.

Implementing CIA at the Application Level

Authentication methods, user roles and accounts, and data encryption are key elements of the application security layer. These elements must be in place to ensure that only authorized users have access to the organization's applications and data and that their access is limited to actions that are consistent with their defined roles and responsibilities.

Authentication Methods

For many applications, users are required to enter a username and password to gain access. This is a form of single-factor authentication as the user needs to provide just one credential, a password to gain access. Two-factor authentication requires the user to provide two types of credential before being able to access an account; the two credentials can be any of the following:

- Something you know, such as a PIN or password
- Something you have, such as some form of security card or token
- Something you are, such as a biometric (for example, a fingerprint or retina scan)

Two-factor authentication is required to withdraw money from a cash machine. You must present your bank card (something that you have) and a PIN (something that you know) to obtain cash from the machine.

User Roles and Accounts

Another important safeguard at the application level is the creation of roles and user accounts so that once users are authenticated, they have the authority to perform their responsibilities and nothing more. For example, members of the finance department should have different authorizations from members of the human resources department. An accountant should not be able to review the pay and attendance records of an employee, and a member of the human resources department should not know how much was spent to modernize a piece of equipment. Even within one department, not all members should be given the same capabilities. Within the accounting department, for example, some users may be able to approve invoices for payment, but others may only be able to enter them. An effective system administrator will identify the similarities among users and create profiles associated with these groups.

Data Encryption

Major enterprise systems such as enterprise resource planning (ERP), customer relationship management (CRM), and product lifecycle management (PLM) access sensitive data residing on data storage devices located in data centers, in the cloud, or at third-party locations. Data encryption should be used within such applications to ensure that these sensitive data are protected from unauthorized access.

Implementing CIA at the End-User Level

Security education, authentication methods, antivirus software, and data encryption must all be in place to protect what is often the weakest link in the organization's security perimeter—the individual end-user.

Security Education

Creating and enhancing user awareness of security policies is an ongoing security priority for companies. Employees and contract workers must be educated about the importance of security so that they will be motivated to understand and follow security policies. This can often be accomplished by discussing recent security incidents that affected the organization. Users must understand that they are a key part of the security system and that they have certain responsibilities. For example, users must help protect an organization's information systems and data by doing the following:

- Guarding their passwords to protect against unauthorized access to their accounts
- Prohibiting others from using their passwords

- Applying strict access controls (file and directory permissions) to protect data from disclosure or destruction
- Reporting all unusual activity to the organization's IT security group
- Taking care to ensure that portable computing and data storage devices are protected (hundreds of thousands of laptops are lost or stolen per year)

Table 3-5 provides a simple self-assessment security test that employees and contractors alike should be asked to complete.

TABLE 3-5 Self-assessment security test

Security assessment question
Do you have the most current version of your computer's operating system installed?
Do you have the most current version of firewall, antivirus, and malware software installed?
Do you install updates to all your software when you receive notice that a new update is available?
Do you use different, strong passwords for each of your accounts and applications—a minimum of 10 characters, with a mix of capital and lowercase letters, numbers, and special characters?
Are you familiar with and do you follow your organization's policies in regard to accessing corporate websites and applications from your home or remote locations (for example, access via a VPN)?
Have you set the encryption method to WPA2 and changed the default name and password on your home wireless router?
When using a free, public wireless network, do you avoid checking your email or accessing websites requiring a username and password?
Do you refrain from clicking on a URL in an email from someone you do not know?
Do you back up critical files to a separate device at least once a week?
Are you familiar with and do you follow your organization's policies regarding the storage of personal or confidential data on your device?
Does your device have a security passcode that must be entered before it accepts further input?
Have you installed Locate My Device or similar software in case your device is lost or stolen?
Do you make sure not to leave your device unattended in a public place where it can be easily stolen?
Have you reviewed and do you understand the privacy settings that control who can see or read what you do on Facebook and other social media sites?

Authentication Methods

End users should be required to implement a security passcode that must be entered before their computing/communications device accepts further input. If your device supports Touch ID, you can use your fingerprint instead of your passcode. Again, a number of multifactor authentication schemes can be used.

Antivirus Software

Antivirus software should be installed on each user's personal computer to scan a computer's memory and disk drives regularly for viruses. Antivirus software scans for a specific sequence of bytes, known as a **virus signature**, that indicates the presence of a specific virus. If it finds a virus, the antivirus software informs the user, and it may clean, delete, or quarantine any files, directories, or disks affected by the malicious code. Good antivirus software checks vital system files when the system is booted up, monitors the system continuously for virus-like activity, scans disks, scans memory when a program is run, checks programs when they are downloaded, and scans email attachments before they are opened. Two of the most widely used antivirus software products are Norton AntiVirus from Symantec and Personal Firewall from McAfee.

According to US-CERT, most virus and worm attacks use already known malware programs. Thus, it is crucial that antivirus software be continually updated with the latest virus signatures. In most corporations, the network administrator is responsible for monitoring network security websites frequently and downloading updated antivirus software as needed. Many antivirus vendors recommend—and provide for—automatic and frequent updates. Unfortunately, antivirus software is not able to identify and block all viruses.

Data Encryption

While you should already have a login password for your mobile computing device or workstation, those measures won't protect your data if someone steals your device—the thief can simply remove your storage device or hard drive and plug it into another computing device and access the data. If you have sensitive information on your computer, you need to employ full-disk encryption, which protects all your data even if your hardware falls into the wrong hands.

CRITICAL THINKING EXERCISE: HOW SECURE IS YOUR ORGANIZATION?

Review and answer the security questions in Table 3-5. Based on this self-assessment, what changes do you need to make in order to better protect the security of your (or your organization's) information systems and data?

RESPONSE TO CYBERATTACK

An organization should be prepared for the worst—a successful attack that defeats all or some of a system's defenses and damages data and information systems. A response plan should be developed well in advance of any incident and be approved by both the organization's legal department and senior management. A well-developed response plan helps keep an incident under technical and emotional control.

In a security incident, the primary goal must be to regain control and limit damage, not to attempt to monitor or catch an intruder. Sometimes system administrators take the discovery of an intruder as a personal challenge and lose valuable time that should be used to restore data and information systems to normal.

Incident Notification

A key element of any response plan is to define who to notify and who not to notify in the event of a computer security incident. Questions to cover include the following: Within the company, who needs to be notified, and what information does each person need to have? Under what conditions should the company contact major customers and suppliers? How does the company inform them of a disruption in business without unnecessarily alarming them? When should local authorities or the FBI be contacted?

Most security experts recommend against giving out specific information about a compromise in public forums, such as news reports, conferences, professional meetings, and online discussion groups. All parties working on the problem must be kept informed and up-to-date without using systems connected to the compromised system. The intruder may be monitoring these systems and emails to learn what is known about the security breach.

A critical ethical decision that must be made is what to tell customers and others whose personal data may have been compromised by a computer incident. Many organizations are tempted to conceal such information for fear of bad publicity and loss of customers. Because such inaction is perceived by many to be unethical and harmful, a number of state and federal laws have been passed to force organizations to reveal when customer data have been breached.

Protection of Evidence and Activity Logs

An organization should document all details of a security incident as it works to resolve the incident. Documentation captures valuable evidence for a future prosecution and provides data to help during the incident eradication and follow-up phases. It is especially important to capture all system events, the specific actions taken (what, when, and who), and all external conversations (what, when, and who) in a logbook. Because this may become court evidence, an organization should establish a set of document-handling procedures using the legal department as a resource.

Incident Containment

Often, it is necessary to act quickly to contain an attack and to keep a bad situation from becoming even worse. The incident response plan should clearly define the process for deciding if an attack is dangerous enough to warrant shutting down or disconnecting critical systems from the network. How such decisions are made, how fast they are made, and who makes them are all elements of an effective response plan.

Eradication

Before the IT security group begins the eradication effort, it must collect and log all possible criminal evidence from the system and then verify that all necessary backups are current, complete, and free of any malware. Creating a forensic disk image of each compromised system on write-only media both for later study and as evidence can be very useful. After virus eradication, a new backup must be created. Throughout this process, a log should be kept of all actions taken. This will prove helpful during the incident follow-up phase and ensure that the problem does not recur. It is imperative to back up critical applications and data regularly. Many organizations, however, have implemented inadequate backup processes and found that they could not fully restore original data after a security incident. All backups should be created with enough frequency to enable a full and quick restoration of data if an attack destroys the original, and this process must be tested to confirm that it works.

Incident Follow-Up

Of course, an essential part of follow-up is to determine how the organization's security was compromised so that it does not happen again. Often the fix is as simple as getting a software patch from a product vendor. However, it is important to look deeper than the immediate fix to discover why the incident occurred. If a simple software fix could have prevented the incident, then why wasn't the fix installed before the incident occurred?

A review should be conducted after an incident to determine exactly what happened and to evaluate how the organization responded. One approach is to write a formal incident report that includes a detailed chronology of events and the impact of the incident. This report should identify any mistakes so that they are not repeated in the future. The experience from this incident should be used to update and revise the security incident response plan. The key elements of a formal incident report should include the following:

- IP address and name of host computer(s) involved
- The date and time when the incident was discovered
- How the incident was discovered
- The method used to gain access to the host computer
- A detailed discussion of vulnerabilities that were exploited
- A determination of whether or not the host was compromised as a result of the attack
- The nature of the data stored on the computer (customer, employee, financial, etc.)
- A determination of whether the accessed data are considered personal, private, or confidential
- The number of hours the system was down
- The overall impact on the business
- An estimate of total monetary damage from the incident
- A detailed chronology of all events associated with the incident

Creating a detailed chronology of all events will also document the incident for possible later prosecution. To this end, it is critical to develop an estimate of the monetary damage. Potential costs include loss of revenue, loss in productivity, and the salaries of people working to address the incident, along with the cost to replace data, software, and hardware.

Another important issue is the amount of effort that should be put into capturing the perpetrator. If a website was simply defaced, it is easy to fix or restore the site's HTML (Hypertext Markup Language—the code that describes to your browser how a web page should look). However, what if the intruders inflicted more serious damage, such as erasing proprietary program source code or the contents of key corporate databases? What if they stole company trade secrets? Expert crackers can conceal their identity, and tracking them down can take a long time as well as a tremendous amount of corporate resources.

The potential for negative publicity must also be considered. Public discussion of security attacks through public trials and the associated publicity has not only enormous potential costs in public relations but real monetary costs as well. For example, a bank or a brokerage firm might lose customers who learn of an attack and think their money or records aren't secure. Even if a company decides that the negative publicity risk is worth it and goes after the perpetrator, documents containing proprietary information that must be provided to the court could cause even greater security threats in the future. On the other hand, an organization must consider whether it has an ethical or a legal duty to inform customers or clients of a cyberattack that may have put their personal data or financial resources at risk.

Using an MSSP

Keeping up with computer criminals—and with new laws and regulations—can be daunting for organizations. Criminal hackers are constantly poking and prodding, trying to breach the security defenses of organizations. Also, laws such as HIPAA, Sarbanes-Oxley, and the USA Patriot Act require businesses to prove that they are securing their data. For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations is too costly to acquire and maintain. As a result, many organizations outsource their network security operations to a **managed security service provider (MSSP)**, which is a company that monitors, manages, and maintains computer and network security for other organizations. MSSPs include such companies as AT&T, Computer Sciences Corporation, Dell SecureWorks, IBM, Symantec, and Verizon. MSSPs provide a valuable service for IT departments drowning in reams of alerts and false alarms coming from VPNs; antivirus, firewall, and IDSs; and other security-monitoring systems. In addition, some MSSPs provide vulnerability scanning and web blocking and filtering capabilities.

Computer Forensics

Computer forensics is a discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law. A computer forensics investigation may be opened in response to a criminal investigation or civil litigation. It may also be launched for a variety of other reasons, for example, to retrace steps taken when data have been lost, to assess damage following a computer incident, to investigate the unauthorized disclosure of personal or corporate confidential data, or to confirm or evaluate the impact of industrial espionage.

Computer forensics investigators work as a team to investigate an incident and conduct forensic analysis by using various methodologies and tools to ensure the computer network system is secure in an organization. For example, accounting, tax, and advisory company Grant Thornton International has a number of IT labs around the world that employ forensic experts who examine digital evidence for use in legal cases. To support its investigators, Grant Thornton has deployed forensic software called Summation (a web-based legal document, electronic data, and transcript review platform that supports litigation teams) and Forensic Toolkit (used to scan a hard drive to find a variety of information, including deleted emails and text strings, to crack encryption). These two applications provide Grant Thornton a combination of mobile forensics, computer forensics, and functions for encoding and reviewing multilingual documents.[46]

Proper handling of a computer forensics investigation is the key to fighting computer crime successfully in court. In addition, extensive training and certification increases the stature of a computer forensics investigator in a court of law. Numerous certifications relate to computer forensics, including the CCE (Certified Computer Examiner), CISSP (Certified Information Systems Security Professional), CSFA (CyberSecurity Forensic Analyst), and GCFA (Global Information Assurance Certification Certified Forensics Analyst). The EnCE Certified Examiner program certifies professionals who have mastered computer investigation methods as well as the use of Guidance Software's EnCase computer forensic software. Numerous universities (both online and traditional) offer degrees specializing in computer forensics. Such degree programs should include training in accounting, particularly auditing, as this is very useful in the investigation of cases involving fraud.

Table 3-6 provides a manager's checklist for evaluating an organization's readiness to prevent and respond to a cyberattack.

TABLE 3-6 Manager's checklist for assessing an organization's readiness to prevent and respond to a cyberattack

Question
Has a risk assessment been performed to identify investments in time and resources that can protect the organization from its most likely and most serious threats?
Have senior management and employees involved in implementing security measures been educated about the concept of reasonable assurance?
Has a security policy been formulated and broadly shared throughout the organization?
Have automated systems policies been implemented that mirror written policies?
Does the security policy address the following? • Email with executable file attachments • Wireless networks and devices • Use of smartphones deployed as part of corporate rollouts as well as those purchased by end users
Is there an effective security education program for employees and contract workers?
Has a multi-layered CIA security strategy been implemented?
Has a firewall been installed?
Is antivirus software installed on all personal computers?
Is the antivirus software frequently updated?
Have precautions been taken to limit the impact of malicious insiders?
Are the accounts, passwords, and login IDs of former employees promptly deleted?
Are employee responsibilities adequately defined and separated?
Are individual roles defined so that users have authority to perform their responsibilities and nothing more?
Is it a requirement to review at least quarterly the most critical Internet security threats and implement safeguards against them?
Has it been verified that backup processes for critical software and databases work correctly?
Has an intrusion detection system been implemented to catch intruders in the act—both in the network and on critical computers on the network?
Are periodic IT security audits conducted?
Has a comprehensive incident response plan been developed?
Has the security plan been reviewed and approved by legal and senior management?
Does the plan address all of the following areas? • Incident notification • Protection of evidence and activity logs • Incident containment • Eradication • Incident follow-up

CRITICAL THINKING EXERCISE: SELECTING AN MSSP PROVIDER

Your team has been assigned responsibility to identify an appropriate MSSP provider for a small, rural hospital. What criteria will you use to select an appropriate provider? Do research online to identify three MSSP providers. Use the criteria you established to rate each of the three, and choose the one that would be best for the hospital.

Summary

Why are computer incidents so prevalent, and what are their effects?

- Increasing computing complexity, expanding and changing systems, an increase in the prevalence of BYOD policies, a growing reliance on software with known vulnerabilities, and the increasing sophistication of those who would do harm have caused a dramatic increase in the number, variety, and severity of security incidents.
- An exploit is an attack on an information system that takes advantage of a particular system vulnerability. Often this attack is due to poor system design or implementation.
- Many different types of people launch computer attacks, including the black hat hacker, cracker, malicious insider, industrial spy, cybercriminal, hacktivist, and cyberterrorist. Each type has a different motivation.
- A white hat hacker is someone who has been hired by an organization to test the security of its information systems allowing the organizations to improve its defenses.
- Ransomware, viruses, worms, Trojan horses, logic bombs, blended threats, spam, DDoS attacks, rootkits, advanced persistent threats, phishing, spear phishing, smishing, vishing, cyberespionage, and cyberterrorism are among the most common computer exploits.
- The DHS has the responsibility to provide for a "safer, more secure America, which is resilient against terrorism and other potential threats." The agency's Office of Cybersecurity and Communications is responsible for enhancing the security, resilience, and reliability of U.S. cyber and communications infrastructure.
- The US-CERT is a partnership between DHS and the public and private sectors that was established to protect the nation's Internet infrastructure against cyberattacks by serving as a clearinghouse for information on new viruses, worms, and other computer security topics.
- Over the years, several laws have been enacted to prosecute those responsible for computer-related crime, including the Computer Fraud and Abuse Act, the Fraud and Related Activity in Connection with Access Devices Statute, the Stored Wire and Electronic Communications and Transactional Records Access Statutes, and the USA Patriot Act.

What can be done to implement a strong security program to prevent cyberattacks?

- The IT security practices of organizations worldwide must be focused on ensuring confidentiality, maintaining integrity, and guaranteeing the availability of their systems and data. Confidentiality, integrity, and availability are referred to as the CIA security triad.
- An organization's security strategy must include security measures that are planned for, designed, implemented, tested, and maintained at the organization, network, application, and end-user levels.
- Every organization needs a risk-based strategy with an active governance process to minimize the potential impact of any security incident and to ensure business continuity in the event of a cyberattack. Key elements of such a strategy include a risk assessment to identify and prioritize the threats that the organization faces, a well-defined disaster recovery plan that ensures the availability of key data and information technology assets, definition of security policies needed to guide employees to follow recommended processes and practices to avoid security-related problems, periodic security audits to ensure that individuals

are following established policies and to assess if the policies are still adequate even under changing conditions, compliance standards defined by external parties, and use of a security dashboard to help track the key performance indicators of their security strategy.

- The concept of reasonable assurance in connection with IT security recognizes that managers must use their judgment to ensure that the cost of control does not exceed the system's benefits or the risks involved.
- Authentication methods, a firewall, routers, encryption, proxy servers, VPN, and an IDS are key elements of the network security layer.
- Authentication methods, user roles and accounts, and data encryption are key elements of the application security layer.
- Security education, authentication methods, antivirus software, and data encryption are key elements of the end-user security layer.

What actions must be taken in the event of a successful security intrusion?

- No security system is perfect, so systems and procedures must be monitored to detect a possible intrusion. A response plan should be developed well in advance of any incident and be approved by both the organization's legal department and senior management. The response plan should address notification, evidence protection, activity log maintenance, containment, eradication, and follow-up.
- Organizations must implement fixes against well-known vulnerabilities and conduct periodic IT security audits.
- Many organizations outsource their network security operations to a MSSP, which is a company that monitors, manages, and maintains computer and network security for other organizations.
- Organizations must be knowledgeable of and have access to trained experts in computer forensics to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law.

Key Terms

advanced persistent threat (APT)

antivirus software

blended threat

botnet

bring your own device (BYOD)

business continuity plan

CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart)

CIA security triad

computer forensics

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act

cyberespionage

cyberterrorism

Department of Homeland Security (DHS)

disaster recovery plan

distributed denial-of-service (DDoS) attack

encryption

encryption key

exploit

firewall

intrusion detection system (IDS)

logic bomb

managed security service provider (MSSP) mission-critical process

next-generation firewall (NGFW)

phishing

ransomware

reasonable assurance

risk assessment

rootkit

security audit

security policy

smishing

spam

spear phishing

Transport Layer Security (TLS)

Trojan horse

U.S. Computer Emergency Readiness Team (US-CERT)

virus

virus signature

vishing

worm

zero-day exploit

zombie

Self-Assessment Questions

Why are computer incidents so prevalent, and what are their effects?

1. The number of global companies that have an overall security strategy is __________.
   a. less than one-third
   b. more than two-thirds
   c. about 58 percent
   d. nearly 75 percent
2. The worldwide financial services industry spent over $27 billion on IT security and fraud prevention in 2015. True or False?
3. A(n) __________ is an attack on an information system that takes advantage of a particular system vulnerability.
   a. virus
   b. worm
   c. Trojan horse
   d. exploit
4. A(n) __________ exploit is an attack that takes place before the security community and/or software developers become aware of and fix a security vulnerability.
5. A(n) __________ is an individual who hacks computers or websites in an attempt to promote a political ideology.
   a. black hat hacker
   b. cracker
   c. malicious insider
   d. hacktivist
6. A(n) __________ is a sophisticated threat that combines the features of a virus, worm, Trojan horse, and other malicious code into a single payload.

7. A(n) ______________ is an attack in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks.
   a. rootkit
   b. zombie
   c. botnet
   d. distributed denial-of-service
8. ______________ is an exploit in which victims receive a voice-mail message telling them to call a phone number or access a website.
9. ______________ involves the deployment of malware that secretly steals data in the computer systems of organizations that can be used to gain an unfair competitive advantage for the perpetrator.
   a. Cyberterrorism
   b. Data breach
   c. Cyberespionage
   d. Smishing

What Can be Done to Implement a Strong Security Program to Prevent Cyberattacks?

10. The computer security triad consists of ______________.
    a. security, confidentiality, and intelligence
    b. confidence, safety, and integrity
    c. confidence, safety, and intelligence
    d. integrity, confidentiality, and availability
11. ______________ is the process of assessing security-related risks to an organization's computers and networks from both internal and external threats.
12. The business recovery plan is the documented process to recover an organization's business information system assets including hardware, software, data, networks, and facilities in the event of a disaster. True or False?
13. Which of the following is not a multifactor authentication method?
    a. Entering a user name and a strong end-user password at least 10 characters long including capital letters, numbers, and special characters
    b. Plugging a hardware token into a USB port of the computer and entering an end-user password
    c. Entering a password and providing a voice pattern sample
    d. Providing a fingerprint recognition and entering a password

14. A(n) ______________ is a hardware- or software-based network security system that is able to detect and block sophisticated attacks by filtering network traffic depend on the contents of data packets.
    a. firewall
    b. router
    c. antivirus software
    d. next-generation firewall

15. ______________ is the process of scrambling messages or data in such a way that only authorized parties can read it.

16. A virtual private network (VPN) enables remote users to securely access an organization's collection of computing and storage devices and share data remotely transmitting and receiving data over public networks such as the Internet. True or False?

17. Antivirus software scans for a specific sequence of bytes known as a(n) ______________ that indicates the presence of a specific virus.

What Actions Must be Taken in the Event of a Successful Security Intrusion?

18. In the event of a successful cyberattack, the best way to give out specific information is through use of online discussion groups, email, and other systems connected to the compromised system. True or False?

19. A(n) ______________ is a company that monitors, manages, and maintains computer and network security for other organizations.

20. ______________ is a discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer system, networks, and storage devices in a manner that preserves the integrity of data gathered so that it is admissible as evidence in a court of law.

Self-Assessment Answers

1. c; 2. True; 3. d; 4. zero-day; 5. d; 6. blended threat; 7. d; 8. Vishing; 9. c; 10. d; 11. Risk assessment; 12. False; 13. a; 14. d; 15. Encryption; 16. True; 17. virus signature; 18. False; 19. managed security service provider (MSSP); 20. Computer forensics

Discussion Questions

1. Imagine that you are designing a smishing scam that involves sending text to people to entice them to go to a website and provide personal information that you can use to access their checking account. Craft a text message that would be difficult for people to ignore. Design a simple web page that would look legitimate to people who bank at your bank and that would capture their checking account number and PIN.
2. A successful DDoS attack requires the downloading of software that turns unprotected computers into zombies under the control of the malicious hacker. Should the owners of the zombie computers be tracked down, identified, and fined or otherwise punished as a means of encouraging people to better safeguard their computers? Why or why not?

3. Briefly describe the difference between a risk assessment and an IT security audit.
4. Identify and briefly discuss a real-world example of a legitimate organization using spam in an effective and nonintrusive manner to promote a product or service.

5. Briefly describe the difference between reasonable assurance and risk assessment.
6. Some IT security personnel believe that their organizations should employ former computer criminals who now claim to be white hat hackers to identify weaknesses in their organizations' security defenses. Do you agree? Why or why not?
7. The National Security Agency (NSA) works to detect and prevent threats to National Security Systems, which includes systems that handle classified information or are otherwise critical to military or intelligence activities. The NSA plays a vital role in our national security by providing America's leaders with critical information they need to defend our country, save lives, and advance U.S. goals and alliances globally. Tailored Access Operations (TAO) is a group of super hackers within the NSA that collects intelligence about foreign targets by breaking into their computers, stealing data, and monitoring communications. TAO is also responsible for developing programs that could destroy or damage foreign computers and networks via cyberattacks if commanded to do so by the president. What sort of personal characteristics would be important in selecting a candidate for the NSA super-secret Tailored Access Operations organization? What would be some of the pros and cons of such a position? Would you consider taking such a position? Why or why not?
8. Hundreds of a bank's customers have called the customer service call center to complain that they are receiving text messages on their phone telling them to access a website and enter personal information to resolve an issue with their account. What action should the bank take?
9. How would you distinguish between a hacktivist and a cyberterrorist? Should the use of hacktivists by a country against enemy organizations be considered an act of war? Why or why not? How about the use of cyberterrorists?

What Would You Do?

Use the five-step decision-making process discussed in Chapter 1 to analyze the following situations and recommend a course of action.

1. You and your team have been hired to assess the computer security of a small retailer. Where would you begin your assessment? What would you look for?
2. It appears that someone is using your firm's corporate directory—which includes job titles, email addresses, and phone numbers—to contact senior managers and directors via text message. The text message requests that the recipient click on a URL, which leads to a website that looks as if it were designed by your human resources organization. Once at this phony website, the employees are asked to enter their bank routing number and account number to be used for electronic deposit of their annual bonus check. You are a member of the IT security group for the firm. What can you do?
3. You are the manager of the IT organization of a small business. The owner calls you late one night and tells you that she just received an anonymous call demanding payment of

$10,000 or the company's customer database will be encrypted and made inaccessible by a logic bomb that has already been planted in the firm's billing system. What do you say? What can you do?

4. Your classmate tells you that he has been working all semester to create a blended threat and that he plans to test it against the university's computer systems this weekend. What do you say?
5. You are one of the top students in your university's computer science program of 100 students, and you have agreed to meet with a recruiter from the Department of Homeland Security. Over dinner, he talks to you about the increasing threat of cyberterrorist attacks launched on the United States by foreign countries and the need to counter those attacks. The agency has a strong need for people who can both develop and defend against zero-day exploits that could be used to plant malware in the software used by the government and military computers. At the end of the dinner, the recruiter asks, "Would such a role be of interest to you?" How do you respond?
6. You are a computer security trainer for your firm's 200 employees and contract workers. What are the key topics you would cover in your initial half-hour basic training program on security for non-IT personnel? What sort of additional security-related training might be appropriate once people have the basics covered?

Cases

1. Fairplay Turns to a Managed Security Service Provider

Fairplay Finer Foods is an independent grocery retailer that operates in the greater Chicago area. From its beginning, Fairplay's mission has been to provide quality foods at an affordable price along with exceptional customer service. Starting with a single store in 1975, Fairplay has since grown to seven locations. The opening of each new store led to increased sales and attracted new customers; however, expansion also raised new information system needs as well as information security risks.

Due to its size, it was not practical for Fairplay to create and run its own information technology organization, so it contracted with KCS Computer Technology, Inc., to provide these services along with the necessary computer hardware and systems. One of KCS's key accomplishments for Fairplay was to implement and manage a corporate network that the grocery chain uses to run applications and communicate across all of its stores.

Another important area of focus for KCS involved helping Fairplay manage issues related to the Payment Card Industry Data Security Standard (PCI DSS). Retailers accepting credit cards and other forms of electronic payment are required to comply with the PCI DSS. The PCI DSS standard ensures that businesses follow best practices for protecting their customers' payment card information. The necessity to comply with the PCI DSS standard along with concern over potential network security issues led Fairplay and KCS to seek out a managed security service provider (MSSP).

After a thorough investigation, Fairplay and KCS selected ControlScan, an MSSP headquartered in Atlanta. This choice was based on ControlScan's simple pricing model, stable of certified security experts, advanced technology, and solid reputation. As part of its contract with

Fairplay, ControlScan agreed to serve as an extension of KCS, delivering cloud-based security technologies and related security support services, including:

- Installing, configuring, and monitoring a system of next-generation firewalls
- Investigating, responding to, and reporting on security-related events
- Providing network usage reports for insights into company resource utilization
- Upgrading the network on an ongoing basis by implementing the latest security enhancements
- Providing expertise to reduce network complexity and contain network-related costs

ControlScan's initial project was installing next-generation firewall appliances to protect each of Fairplay's locations. This work was completed overnight in a single night to minimize business disruption. ControlScan then conducted a thorough PCI gap analysis to compare current Fairplay security controls with those required by the PCI DSS. ControlScan developed a detailed set of recommendations and options for eliminating the gaps, giving Fairplay management a roadmap to achieve full PCI DSS compliance. Finally, ControlScan did a full review of all of Fairplay's existing information systems and security policies, working with the chain's IT staff to tweak and customize policies where necessary.

Critical Thinking Questions

1. What advantages does the use of an MSSP offer a small retailer such as Fairplay? Can you think of any potential drawbacks of this approach? Is there a danger in placing too much trust in an MSSP? Explain.
2. Data breaches at major retailers, such as Neiman Marcus, Target, and others, in recent years have shown that compliance with the PCI DSS is no guarantee against an intrusion (see Jaikumar Vijayan, "After Target, Neiman Marcus Breaches, Does PCI Compliance Mean Anything?," *Computerworld*, January 24, 2014). If you were a member of Fairplay's management team, what additional actions would you take to protect your customer's credit card data?
3. Do research online to gain insight into the evolution of the PCI DSS standard. What major changes were made in moving from PCI 2.0 to PCI 3.0? What changes are being suggested for future versions of the PCI standard?

Sources: "About Fairplay," Fairplay, www.fairplayfoods.com/about (accessed April 12, 2016); "KCS Computer Technology," KCS Computer Technology, Inc., www.kcstech.com (accessed March 12, 2016); "Fairplay Finer Foods Secures Chain Stores with ControlScan Managed Security Services," ControlScan, www.controlscan.com/fairplay-finer-foods-secures-chain-stores-with-controlscan-managed-security-services (accessed April 12, 2016); "PCI FAQs," PCI Compliance Guide, www.pcicomplianceguide.org/pci-faqs-2/#1 (accessed April 12, 2016).

2. Sony's Response to North Korea's Cyberattack

On November 24, 2014, employees of Sony Pictures Entertainment booted up their computers to find an image of a skull along with a message from a group calling itself the Guardians of Peace. The message read: "We've already warned you and this is just the beginning. We've obtained all your internal data including your secrets and top secrets [which will be released] if you don't obey us."

As Sony would eventually discover, the hackers had stolen reams of sensitive data, including the Social Security numbers of 47,000 current and former employees, system passwords, salary lists, contracts, and even copies of some Sony employees' passports. The hackers accessed hundreds of Outlook mailboxes as well as Sony IT audit documents. They also stole media files and placed pirated copies of five of Sony's movies on illegal file-sharing servers. Sony was forced to completely shut down its information systems in an attempt to stem the data breach. Ultimately, Sony would determine that the damage done by the hackers was far more extensive than it first believed. Not only had data been stolen, but 75 percent of the company's servers had been destroyed and several internal data centers had been wiped clean.

Contacted within hours of the event, the FBI soon identified the culprit. In June, several months before the hack, North Korea's Ministry of Foreign Affairs had declared that it would take "a decisive and merciless countermeasure" if the U.S. government did not prevent the planned release of Sony's motion picture *The Interview*, which features two reporters who venture to North Korea to interview and assassinate the country's dictator, Kim Jong-un. In the film, the main character, initially won over by the dictator's apparent kindness, discovers that the tyrant is lying about the country's prosperity and freedoms. The plot, along with the movie's unflattering portrayal of the dictator as ruthless and childish, had caught the attention of the North Korean government.

The U.S. government disclosed that it had proof that the North Koreans had made good on their threat. The U.S. National Security Agency (NSA) had reportedly penetrated the North Korean cyberwarfare unit four years prior to the attack and had been monitoring its capabilities since then. After Sony alerted the FBI of the attack, the NSA was able to trace the attack back to North Korea, using a digital fingerprint the hackers had left in the malware. Several weeks after the attack, FBI Director James Comey revealed in a speech that the Sony hackers had been sloppy. "We could see that the IP [Internet protocol] addresses that were being used to post and to send the emails were coming from IPs that were exclusively used by the North Koreans."

The hackers warned Sony not to release *The Interview*, and then on December 16, the group issued a message threatening large terrorist attacks on theaters that showed the film. The National Organization of Theatre Owners contacted the Department of Homeland Security for information and advice. The FBI and NSA released a bulletin explaining that they had no credible information about a plan to attack theaters, but they could neither confirm nor deny whether the hackers had the ability to launch such an attack. Shortly after the bulletin was released, the four largest U.S. theater chains withdrew their requests to show the movie—Carmike Cinemas first, followed by Regal Entertainment, AMC Entertainment, and Cinemark. Within hours, Sony announced that it had canceled the film's release. White House officials, Hollywood personalities, and the media were aghast. Comedian Jimmy Kimmel tweeted that the decision by the major theater chains to refuse to screen *The Interview* was "an un-American act of cowardice that validates terrorist actions and sets a terrifying precedent."

On December 19, President Obama addressed the issue publicly: "Sony is a corporation. It suffered significant damage. There were threats against its employees. I'm sympathetic to the concerns that they faced. Having said all that, yes, I think they made a mistake." Obama explained, "We cannot have a society in which some dictator in some place can start imposing censorship in the United States." The president's remarks highlighted the seriousness of the incident to the American public, many of whom came to view the incident as an attack on the freedom of expression.

In response to Obama's comments, Sony officials released a statement later the same day: "Let us be clear—the only decision that we have made with respect to release of the film was not to release it on Christmas Day in theaters, after the theater owners declined to show it…. After that decision, we immediately began actively surveying alternatives to enable us to release the movie on a different platform. It is still our hope that anyone who wants to see this movie will get the opportunity to do so."

In fact, on Christmas Day, the planned release day in the theater, *The Interview* became available through video-on-demand outlets such as Amazon.com, and within less than a month, the movie had brought in over $40 million in revenue. Approximately 6 million viewers had rented or purchased the movie in this way. Several hundred movie theaters that opted to screen the movie generated another $6 million. Over the next two months, Sony also released the movie on Netflix, on DVD and Blu-ray, and in theaters in other countries.

Sony has worked to recover from the damage done to the company itself by the hack. Sony Pictures' parent company, which is based in Japan, asked regulators there for an extension to file its 2015 third-quarter financial results. It also fired executive Amy Pascal whose leaked emails contained derogatory remarks about Hollywood producers and the U.S. president's movie preferences. The company also provided one year of free credit protection services to current and former employees.

In February 2015, President Obama held the first-ever White House summit on cybersecurity issues in Silicon Valley. The summit was billed as an attempt to deal with the increasing vulnerability of U.S. companies to cyberattacks—including those backed by foreign governments. However, the chief executives of Microsoft, Google, Facebook, and Yahoo all refused to attend the summit. Those companies have long advocated for the government to stop its practice of collecting and using private data to track terrorist and criminal activities and have worked to find better ways to encrypt the data of their customers. However, U.S. security agencies have continually pressured the IT giants to keep the data as unencrypted as possible to facilitate the government's law enforcement work. Ultimately, both the government and private businesses will need to find a way to work together to meet two contradictory needs—the country's need to make itself less vulnerable to cyberattacks while at the same time protecting itself from potential real-world violence.

Critical Thinking Questions

1. Do you think that Sony's response to the attack was appropriate? Why or why not?
2. What might Sony and the U.S. government have done differently to discourage future such attacks on other U.S. organizations?
3. Are there measures that organizations and the U.S. government can take together to prevent both real-world terrorist violence and cyberattacks?

Sources: Devlin Barrett and Danny Yadron, "Sony, U.S. Agencies Fumbled After Cyberattack," *Wall Street Journal*, February 22, 2015, www.wsj.com/articles/sony-u-s-agencies-fumbled-after-cyberattack-1424641424; Andrea Mitchell, "Sony Hack: N. Korean Intel Gleaned by NSA During Incursion," *NBC News*, January 18, 2015, www.nbcnews.com/storyline/sony-hack/sony-hack-n-korean-intel-gleaned-nsa-during-incursion-n288761; Amy Schatz, "Obama Acknowledges Strains with

SiliconValley," *SFGate*, February 14, 2015, http://blog.sfgate.com/techchron/2015/02/14/obama-acknowledges-strains-with-silicon-valley/; Devin Dwyer and Mary Bruce, "Sony Hacking: President Obama Says Company Made 'Mistake' in Canceling 'The Interview,'" *ABC News*, December 19, 2014, http://abcnews.go.com/Politics/obama-sony-made-mistake-canceling-film-release/story?id=27720800; Frank Pallotta, "Sony's 'The Interview' Coming to Netflix," *CNN Money*, January 20, 2015, http://money.cnn.com/2015/01/20/media/the-interview-makes-40-million/; Julianne Pepitone, "Sony Hack: 'Critical' Systems Won't Be Back Online until February," *NBC News*, January 23, 2015, www.nbcnews.com/storyline/sony-hack/sony-hack-critical-systems-wont-be-back-online-until-february-n292126; Michael Cieply and Brooks Barnes, "Sony Cyberattack, First a Nuisance, Swiftly Grew into a Firestorm," *New York Times*, December 30, 2014, www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html; "The Interview: A Guide to the Cyber Attack on Hollywood," *BBC*, December 29, 2014, www.bbc.com/news/entertainment-arts-30512032; Zack Whittaker, "FBI Says North Korea Is 'Responsible' for Sony Hack, as White House Mulls Response," *ZDNet*, December 19, 2014, www.zdnet.com/article/us-government-officially-blames-north-korea-for-sony-hack/; Charlie Osborne, "Sony Pictures Corporate Files Stolen and Released in Cyberattack," *ZDNet*, November 28, 2014, www.zdnet.com/article/sony-pictures-corporate-files-stolen-and-released-in-cyberattack; Charlie Osborn, "Sony Hack Exposed Social Security Numbers of Hollywood Celebrities," *ZDNet*, December 5, 2015, www.zdnet.com/article/sony-hack-exposed-social-security-numbers-of-hollywood-celebrities/; David E. Sanger and Nicole Perlroth, "Obama Heads to Tech Security Talks amid Tensions," *New York Times*, February 12, 2015, www.nytimes.com/2015/02/13/business/obama-heads-to-security-talks-amid-tensions.html; Lance Whitney, "Sony Seeks to Delay Filing Earnings in Wake of Cyberattack," *CNET*, January 23, 2015, www.cnet.com/news/sony-asks-to-delay-filing-earnings-due-to-cyberattack.

End Notes

[1] Nicole Perlroth and David E. Sanger, "Nations Buying as Hackers Sell Flaws in Computer Code," *New York Times*, July 13, 2013, www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?_r=0.

[2] Jennifer Markert, "How Zero-Day Exploits Are Bought and Sold in a Murky, Unregulated Market," *Curiousmatic*, February 23, 2015, https://curiousmatic.com/zero-day-exploits.

[3] "Vulnerabilities Equities Process," Electronic Privacy Information Center, https://epic.org/privacy/cybersecurity/vep/default.html (accessed November 10, 2016).

[4] M. Smith, "U.S. Government Is 'Biggest Buyer' of Zero-Day Vulnerabilities, Report Claims," *Network World*, May 12, 2013, www.networkworld.com/article/2224620/microsoft-subnet/u-s–government-is–biggest-buyer–of-zero-day-vulnerabilities–report-claims.html.

[5] Nathan Freed Wessler, "FBI Releases Details of 'Zero-Day' Exploit Decision-Making Process," ACLU, June 26, 2015, https://www.aclu.org/blog/free-future/fbi-releases-details-zero-day-exploit-decisionmaking-process.

[6] Dave Aitel and Matt Tait, "Everything You Know About the Vulnerability Equities Process Is Wrong," *LawFare*, August 18, 2016, https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong.

[7] "Big Data and Predictive Analytics: On the Cybersecurity Frontline," International Data Corporation, August 10, 2015, www.informationweek.com/whitepaper/security-management-&-analytics/cybersecurity/big-data-and-predictive-analytics:-on-the-cybersecurity-front-line/364303?gset=yes&.

[8] "The Global State of Information Security Survey 2016," PwC, www.pwc.com/gx/en/issues/cyber-security/information-security-survey/industry.html (accessed April 16, 2016).

[9] "The Global State of Information Security Survey 2016," PwC, www.pwc.com/gx/en/issues/cyber-security/information-security-survey/industry.html (accessed April 16, 2016).

[10] National Vulnerability Database, https://web.nvd.nist.gov/view/vuln/statistics (accessed September 22, 2016).

[11] Warwick Ashford, "US Hospital Pays £12,000 to Ransomware Attackers," *Computer Weekly*, February 18, 2016, www.computerweekly.com/news/4500273343/US-hospital-pays-12000-to-ransomware-attackers.

[12] Dancho Danchev, "Cornficker's Estimated Economic Cost? $9.1 Billion," *ZDNet*, April 23, 2009, www.zdnet.com/blog/security/confickers-estimated-economic-cost-9-1-billion/3207.

[13] Pelin Aksoy and Laura Denardis, *Information Technology in Theory* (Boston: Cengage Learning, 2007), pp. 299–301.

[14] Jack Cloherty and Pierre Thomas, "?Trojan Horse' Bug Lurking in Vital US Computers Since 2011," *ABC News*, November 6, 2014, http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476.

[15] Matthew J. Schwartz, "How South Korean Bank Malware Spread," *InformationWeek*, March 25, 2013, www.darkreading.com/attacks-and-breaches/how-south-korean-bank-malware-spread/d/d-id/1109239?

[16] Nick Johnston, "Short, Sharp Spam Attacks Aiming to Spread Dyre Financial Malware," Symantec, January 28, 2015, www.symantec.com/connect/blogs/short-sharp-spam-attacks-aiming-spread-dyre-financial-malware.

[17] "Spam Statistics for the Week Ending January 18, 2015," Trustwave, www3.trustwave.com/support/labs/spam_statistics.asp.

[18] Paul Sawers, "Mass Internet Disruption Caused by DDoS Attack on DNS Company Dyn," Venture Beat, October 21, 2017, http://venturebeat.com/2016/10/21/dyn-dyn-dyn-internet-ddos-attack-back-up/.

[19] Kim Kalunian, "2012 Rootkit Computer Virus 'Worst in Years'," *Warwick Beacon*, December 20, 2011, www.warwickonline.com/stories/2012-rootkit-computer-virus-worst-in-years,65964.

[20] Margaret Rouse, "Advanced Persistent Threat," *TechTarget*, http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT (accessed February 17, 2015).

[21] "Advanced Persistent Threats: How They Work," Symantec, www.symantec.com/theme.jsp?themeid=apt-infographic-1 (accessed February 17, 2015).

[22] "International Hacking Ring Steals up to $1 Billion from Banks," *Economic Times*, February 16, 2015, http://economictimes.indiatimes.com/articleshow/46256846.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

[23] "Fraud Alert: New Phishing Tactics—and How They Impact Your Business," Thawte, https://community.thawte.com/system/files/download-attachments/Phishing%20WP_D2.pdf (accessed March 11, 2015).

[24] Dan Raywood, "Anthem Breach Victims Hit with Yet another Phishing Scam," *Security News*, February 16, 2015, www.itproportal.com/2015/02/16/anthem-breach-victims-hit-yet-another-phishing-scam.

[25] Steve Ragan, "Phishing Attacks Targeting W-2 Data Hit 41 Organizations in Q1 2016," *CSO*, March 24, 2016, www.csoonline.com/article/3048263/security/phishing-attacks-targeting-w-2-data-hit-41-organizations-in-q1-2016.html.

[26] Chris Brook, "Vishing Attacks Are Targeting Dozens of Banks," *Threat Post*, April 29, 2014, https://threatpost.com/vishing-attacks-targeting-dozens-of-banks/105774.

[27] Linda McGlasson, "How to Respond to Vishing Attacks: Bank, State Associations Share Tips for Incident Response Plan," BankInfoSecurity.com, April 26, 2010, www.bankinfosecurity.com/p_print.php?t=a&id=2457.

[28] Michael Kan, "China Counters US Claims with Own Charges of Cyber-Espionage," *PC World*, May 19, 2014, www.pcworld.com/article/2157080/china-counters-us-claims-with-own-charges-of-cyberespionage.html.

[29] Sophia Yan, "Chinese Man Admits to Cyber Spying on Boeing and Other U.S. Firms," *CNN Money*, March 24, 2016, http://money.cnn.com/2016/03/24/technology/china-cyber-espionage-military/index.html.

[30] Secure World News Team, "U.S., China Meet to Talk Cybersecurity," *SecureWorld*, May 13, 2016, https://www.secureworldexpo.com/industry-news/us-china-meet-talk-cybersecurity.

[31] Cheryl Pellerin, "White House Announces Voluntary Cybersecurity Framework," U.S. Department of Defense, February 13, 2015, http://archive.defense.gov/news/newsarticle.aspx?id=121660.

[32] "About DHS," Department of Homeland Security, www.dhs.gov/about-dhs (accessed April 7, 2016).

[33] "Office of Cybersecurity and Communications," Department of Homeland Security, www.dhs.gov/office-cybersecurity-and-communications (accessed April 7, 2016).

[34] "About DHS," Department of Homeland Security, www.dhs.gov/about-dhs (accessed April 8, 2016).

[35] Kim Zetter, "Everything We Know About Ukraine's Power Plant Hack," *Wired*, January 20, 2016, www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack.

[36] H. R. 3162, 107th Cong. (2001), www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf (accessed April 8, 2016).

[37] "RecoverPoint," EMC, www.emc.com/storage/recoverpoint/recoverpoint.htm (accessed June 16, 2015).

[38] "SteelEye LifeKeeper," SteelEye Technology, Inc., www.ha-cc.org/high_availability/components/application_availability/cluster/high_availability_cluster/steeleye_lifekeeper (accessed June 16, 2015).

[39] "NeverFail Application Continuous Availability," VirtualizationAdmin.com, www.virtualizationadmin.com/software/High-Availability/Neverfail-for-VMware-VirtualCenter-.html (accessed June 16, 2015).

[40] Kevin Lonergan, “Can Your Disaster Recovery Plan Save Your Business?” *Information Age*, January 29, 2015, www.information-age.com/top-5-application-security-trends-2015-123458930/.

[41] “Algoma Central Corporation Case Study,” Avaap, www.avaap.com/case-studies (accessed April 12, 2016).

[42] “Authentication in an Internet Banking Environment,” Federal Financial Institutions Examination Council, https://www.ffiec.gov/pdf/auth-its-final%206-22-11%20(ffiec%20formated).pdf (accessed November 14, 2016).

[43] Nicole Lyn Pesce, “MasterCard Will Launch ‘Selfie Pay’ Technology This Summer,” *Daily News*, February 23, 2016, www.nydailynews.com/life-style/mastercard-launch-selfie-pay-technology-summer-article-1.2540983.

[44] “Apple Pay,” Apple, www.apple.com/apple-pay (accessed February 29, 2016).

[45] “Encryption: Securing Our Data, Securing Our Lives,” BSA | The Software Alliance, http://encryption.bsa.org/downloads/BSA_encryption_primer.pdf (accessed October 21, 2016).

[46] “Case Study: Grant Thornton, Global Accounting, Tax and Advisory Company Puts Its Trust in AccessData for Computer Forensics and E-Discovery Solutions,” AccessData, http://accessdata.com/resources/digital-forensics/case-study-grant-thornton-global-accounting-tax-and-advisory-company-puts-i (accessed April 9, 2016).

CHAPTER 4

PRIVACY

QUOTE

When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else.

—David Brin, American science fiction writer

Carsten Reisinger/Shutterstock.com

ORGANIZATIONS BEHAVING BADLY

WhatsApp, an instant messaging app for smartphones, allows users to send text messages, documents, images, videos, user location data, and other data over the Internet to other WhatsApp users, using standard cellular mobile numbers. In the past, WhatsApp has been a strong defender of its users' privacy, employing end-to-end encryption for all messages sent through its service and regularly resisting requests from authorities for data access. As a result, WhatsApp has been the instant messaging app of choice for users who wish to keep their conversations private, including individuals working to expose corruption within organizations and those reporting on the activities of totalitarian governments.

Facebook purchased WhatsApp for $22 billion in 2014. After the sale to Facebook was announced, WhatsApp CEO and cofounder Jan Koum declared that nothing would change with the company's privacy practices. Indeed, Koum posted that "If partnering with Facebook meant that we had to change our values, we wouldn't have done it."[1] This statement has come back to haunt him.

In the fall of 2016, WhatsApp announced that it would begin providing user data—including phone numbers, usage data, and information on devices and operating systems being used—to Facebook and the "Facebook family of companies."[2] According to the company, this information allows Facebook to make better friend suggestions and display more relevant ads to users while also allowing businesses to send messages to users, including appointment reminders, delivery and shipping notifications, and marketing pitches. The policy shift is intended to help WhatsApp generate more revenue and makes economic sense; however, the change has raised concerns over the privacy of users' conversations and identities and has upset users drawn to the app by the company's previous strong stance on privacy.

What trade-offs should social network organizations consider when changing their privacy policy? Must the scales always be tipped in favor of increased revenue?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What is the right of privacy, and what is the basis for protecting personal privacy under the law?
2. What are some of the laws that provide protection for the privacy of personal data, and what are some of the associated ethical issues?
3. What are the various strategies for consumer profiling, and what are the associated ethical issues?
4. What is e-discovery, and how is it being used?
5. Why and how are employers increasingly using workplace monitoring?
6. What are the capabilities of advanced surveillance technologies, and what ethical issues do they raise?

PRIVACY PROTECTION AND THE LAW

The use of information technology in both government and business requires balancing the needs of those who use the information that is collected against the rights and desires of the people whose information is being used.

Information about people is gathered, stored, analyzed, and reported because organizations can use it to make better decisions (see Figure 4-1). Some of these decisions, including whether or not to hire a job candidate, approve a loan, or offer a scholarship, can profoundly affect people's lives. In addition, the global marketplace and intensified competition have increased the importance of knowing consumers' purchasing habits and financial condition. Companies use this information to target marketing efforts to consumers who are most likely to buy their products and services. Organizations also need basic information about customers to serve them better. It is hard to imagine an organization having productive relationships with its customers without having data about them. Thus, organizations want systems that collect and store key data from every interaction they have with a customer.

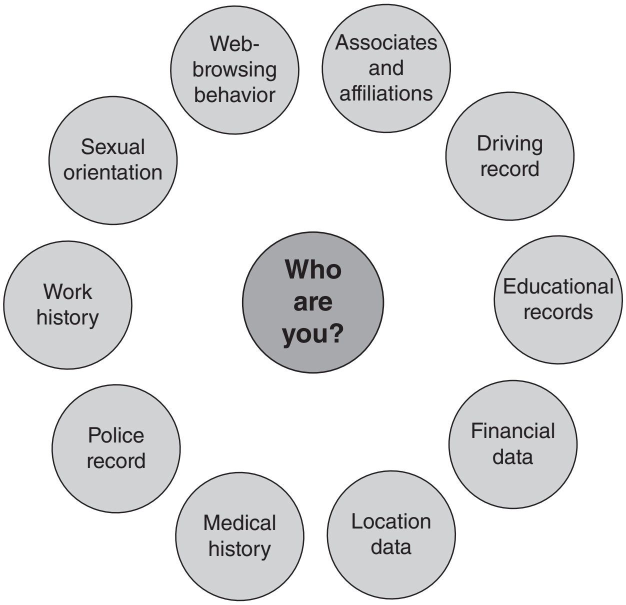


FIGURE 4-1 Organizations gather a variety of data about people in order to make better decisions

However, many people object to the data collection policies of governments and businesses on the grounds that they strip individuals of the power to control their own personal information. For these people, the existing hodgepodge of privacy laws and practices fails to provide adequate protection; rather, it causes confusion that promotes distrust and skepticism, which are further fueled by the disclosure of threats to privacy.

A combination of approaches—new laws, technical solutions, and privacy policies—is required to balance the scales. Reasonable limits must be set on government and business access to personal information; new information and communication technologies must be designed to protect rather than diminish privacy; and appropriate corporate policies must be developed to set baseline standards for people's privacy. Education and communication are also essential.

This chapter will help you understand the right to privacy as well as the developments in information technology that could impact this right. It also addresses a number of ethical issues related to gathering data about people.

First, it is important to gain a historical perspective on the right to privacy. During the debates on the adoption of the U.S. Constitution, some of the drafters expressed concern that a powerful federal government would intrude on the privacy of individual citizens. After the Constitution went into effect in 1789, several amendments were proposed that would spell out additional rights of individuals. Ten of these proposed amendments were ultimately ratified and became known as the **Bill of Rights**. So, although the Constitution does not contain the word *privacy*, the U.S. Supreme Court has ruled that the concept of privacy is protected by the Bill of Rights. For example, the Supreme Court has stated that American citizens are protected by the Fourth Amendment when there is a "reasonable expectation of privacy."

The **Fourth Amendment** reads as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

However, the courts have ruled that without a reasonable expectation of privacy, there is no privacy right.

Today, in addition to protection from government intrusion, people want and need privacy protection from private industry. Few laws provide such protection, and most people assume that they have greater privacy rights than the law actually provides. Some people believe that only those with something to hide should be concerned about the loss of privacy; however, others believe that everyone should be concerned. As the Privacy Protection Study Commission noted in 1977, when the computer age was still in its infancy: "The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable."[3] See Table 4-1.

TABLE 4-1 Systems that gather data about individuals

System/ program	Used by	How used
Automatic license plate readers (ALPRs)	Law enforcement agencies, including the U.S. Drug Enforcement Administration (DEA) and the U.S. Customs and Border Protection agency	ALPRs snap photos and document the location of vehicles; some systems can also photograph drivers and passengers. ALPRs are used to snag red-light runners and to identify motorists with outstanding arrest warrants, overdue parking tickets, and delinquent tax bills.

(*continued*)

TABLE 4-1 Systems that gather data about individuals (*Continued*)

System/ program	Used by	How used
Backscatter imaging scanners	Law enforcement agencies, including the U.S. Customs and Border Protection agency, maritime police, general aviation security, and event security	Backscatter scanners can scan vehicles as well as individuals and crowds at public events to search for currency, drugs, and explosives.
Cookies	For-profit companies, nonprofit organizations, news and social media sites, and most other types of websites	Cookies capture your browsing history for website customization and personalization purposes and for targeted marketing purposes.
Drones	Law enforcement agencies, including the U.S. Customs and Border Protection agency	Drones are unmanned aerial vehicles used to support operations that require aerial surveillance.
Facebook tagging system	Facebook users	Facebook tags identify and reference people in photos and videos posted on Facebook by its more than 1 billion users.
Google location services	Smartphone and other mobile device users	Google's location services store a history of location data from all devices where a user is logged into a Google account.
MYSTIC	National Security Agency (NSA)	MYSTIC is used by the NSA to intercept and record all telephone conversations in certain countries, including Afghanistan, the Bahamas, Mexico, Kenya, and the Philippines. Because there is no practical way to exclude them, the conversations captured by MYSTIC include those of Americans who make calls to or from the targeted countries.[4,5]
PRISM	NSA	PRISM is an NSA surveillance program that collects Internet data, such as search histories; photos sent and received; and the contents of email, file transfers, and voice and video chats. PRISM also gathers data related to telephone calls, including the numbers of both parties on a call and the location, date, time, and duration of the call.
Secure Flight Program	Transportation Security Agency (TSA)	Secure Flight is an airline passenger prescreening program that checks travelers' personal information against the TSA's passenger watch list.
Smart TVs	Some TV manufacturers	Some smart TVs can capture personal conversations along with voice commands used to control the TV via their voice recognition system.
Stingray	Law enforcement agencies	Stingray is a type of hardware device used to impersonate a cell tower, forcing all mobile phones within range to connect to it. The device can then capture information that can be used to identify and locate users and the phone numbers they call or text.
Surveillance cameras	Law enforcement agencies	Cameras are used for intelligence gathering, the prevention of crime, and the protection of individuals or an object, and to support the investigation of a crime.

Many individuals are also concerned about the potential for a data breach in which personal data stored by an organization fall into the hands of criminals.

Information Privacy

A broad definition of the **right of privacy** is "the right to be left alone—the most comprehensive of rights, and the right most valued by a free people."[6] Another concept of privacy that is particularly useful in discussing the impact of IT on privacy is the term information privacy, first coined by Roger Clarke, director of the Australian Privacy Foundation. **Information privacy** is the combination of communications privacy (the ability to communicate with others without those communications being monitored by other persons or organizations) and data privacy (the ability to limit access to one's personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and their use).[7] The following sections cover concepts and principles related to information privacy, beginning with a summary of the most significant privacy laws, their applications, and related court rulings.

Privacy Laws, Applications, and Court Rulings

This section outlines a number of legislative acts that affect a person's privacy. Note that most of these actions address invasion of privacy by the government. Legislation that protects people from data privacy abuses by corporations is almost nonexistent.

Although a number of independent laws and acts have been implemented over time, no single, overarching national data privacy policy has been developed in the United States. Nor is there an established advisory agency that recommends acceptable privacy practices to businesses. Instead, there are laws that address potential abuses by the government, with little or no restrictions for private industry. As a result, existing legislation is sometimes inconsistent or even conflicting. You can track the status of privacy legislation in the United States at the Electronic Privacy Information Center's website (*www.epic.org*).

The discussion is divided into the following topics: financial data, health information, children's personal data, electronic surveillance, fair information practices, and access to government records.

Financial Data

Individuals must reveal much of their personal financial data in order to take advantage of the wide range of financial products and services available, including credit cards, checking and savings accounts, loans, payroll direct deposit, and brokerage accounts. To access many of these financial products and services, individuals must use a personal logon name, password, account number, or PIN. The inadvertent loss or disclosure of these personal financial data carries a high risk of loss of privacy and potential financial loss. Individuals should be concerned about how these personal data are protected by businesses and other organizations and whether or not they are shared with other people or companies.

Fair Credit Reporting Act (1970)

The **Fair Credit Reporting Act** (15 U.S.C. § 1681) regulates the operations of credit reporting bureaus, including how they collect, store, and use credit information. The act, enforced by the U.S. Federal Trade Commission, is designed to ensure the accuracy, fairness, and privacy of information gathered by the credit reporting companies and to provide guidelines for organizations whose systems that gather and sell information about people. The act outlines who may access your credit information, how you can find out what is in your file, how to dispute inaccurate data, and how long data are retained. It also prohibits a credit reporting bureau from giving out information about you to your employer or potential employer without your written consent.[8]

Right to Financial Privacy Act (1978)

The **Right to Financial Privacy Act** (12 U.S.C. § 3401) protects the records of financial institution customers from unauthorized scrutiny by the federal government. Prior to the passage of this act, financial institution customers were not informed if their personal records were being turned over for review by a government authority, nor could customers challenge government access to their records. Under this act, a customer must receive written notice that a federal agency intends to obtain his or her financial records, along with an explanation of the purpose for which the records are sought. The customer must also be given written procedures to follow if he or she does not wish the records to be made available. In addition, to gain access to a customer's financial records, the government must obtain one of the following:

- an authorization signed by the customer that identifies the records, the reasons the records are requested, and the customer's rights under the act;
- an appropriate administrative or judicial subpoena or summons;
- a qualified search warrant or a formal written request by a government agency (can be used only if no administrative summons or subpoena authority is available).

The financial institution cannot release a customer's financial records until the government authority seeking the records certifies in writing that it has complied with the applicable provision of the act.

The act only governs disclosures to the federal government; it does not cover disclosures to private businesses or state and local governments. The definition of financial institution has been expanded to include banks, thrifts, and credit unions; money services businesses; money order issuers, sellers, and redeemers; the U.S. Postal Service; securities and futures industries; futures commission merchants; commodity trading advisors; and casinos and card clubs.

Gramm-Leach-Bliley Act (1999)

The **Gramm-Leach-Bliley Act (GLBA)** (Public Law 106-102), also known as the Financial Services Modernization Act of 1999, was a bank deregulation law that repealed a Depression-era law known as Glass-Steagall.[9] Glass-Steagall prohibited any one institution from offering investment, commercial banking, and insurance services; individual companies were only allowed to offer one of those types of financial service products. GLBA enabled such entities to merge. The emergence of new corporate conglomerates, such as Bank of America, Citigroup, and JPMorgan Chase, soon followed. These one-stop financial supermarkets owned bank branches, sold insurance, bought and sold stocks and bonds, and engaged in mergers and acquisitions. Some people place partial blame for the financial crisis that began in 2008 on the passage of GLBA and the loosening of banking restrictions. GLBA also included three key rules that affect personal privacy:

- *Financial Privacy Rule*—This rule established mandatory guidelines for the collection and disclosure of personal financial information by financial organizations. Under this provision, financial institutions must provide a privacy notice to each consumer that explains what data about the consumer are gathered, with whom that data are shared, how the data are used, and how the data are protected. The notice must also explain the consumer's right to **opt out**—to refuse to give the institution the right to collect and share personal data with unaffiliated parties. Anytime the privacy policy is changed, the consumer must be contacted again and given the right to opt out. The privacy notice must be provided to the consumer at the time the consumer relationship is formed and once each year thereafter. (Section 75001 of the Fixing America's Surface Transportation Act [FAST Act] signed into law in 2015 modified this requirement allowing financial institutions covered under GLBA to be exempt from the annual delivery of privacy notices to customers under certain basic conditions.)[10] Customers who take no action automatically **opt in** and give financial institutions the right to share personal data, such as annual earnings, net worth, employers, personal investment information, loan amounts, and Social Security numbers, with other financial institutions.

- *Safeguards Rule*—This rule requires each financial institution to document a data security plan describing its preparation and plans for the ongoing protection of clients' personal data.
- *Pretexting Rule*—This rule addresses attempts by people to access personal information without proper authority by means such as impersonating an account holder or phishing. GLBA encourages financial institutions to implement safeguards against pretexting.

After the law was passed, financial institutions resorted to mass mailings to contact their customers with privacy-disclosure forms. As a result, many people received a dozen or more similar-looking forms—one from each financial institution with which they did business. However, most people did not take the time to read the long forms, which were printed in small type and full of legalese. Rather than making it easy for customers to opt out, the documents required that consumers send one of their own envelopes to a specific address and state in writing that they wanted to opt out—all this rather than sending a simple prepaid postcard that allowed customers to check off their choice. As a result, most customers threw out the forms without grasping their full implications and thus, by default, agreed to opt in to the collection and sharing of their personal data.

Fair and Accurate Credit Transactions Act (2003)

The **Fair and Accurate Credit Transactions Act** (Public Law 108-159) was passed in 2003 as an amendment to the Fair Credit Reporting Act, and it allows consumers to request and obtain a free credit report once each year from each of the three primary consumer credit reporting companies (Equifax, Experian, and TransUnion). The act also helped establish the National Fraud Alert system to help prevent identity theft. Under this system, consumers who suspect that they have been or may become a victim of identity theft can place an alert on their credit files. The alert places potential creditors on notice that they must proceed with caution when granting credit.[11]

Health Information

The use of electronic medical records and the subsequent interlinking and transferring of this electronic information among different organizations has become widespread. Individuals are rightly concerned about the erosion of privacy of data concerning their health. They fear intrusions into their health data by employers, schools, insurance firms, law enforcement agencies, and even marketing firms looking to promote their products and services. The primary law addressing these issues is the Health Insurance Portability and Accountability Act (HIPAA).

Health Insurance Portability and Accountability Act (1996)

The **Health Insurance Portability and Accountability Act (HIPAA)** (Public Law 104-191) was designed to improve the portability and continuity of health insurance coverage; to reduce fraud, waste, and abuse in health insurance and healthcare delivery; and to simplify the administration of health insurance.

To these ends, HIPAA requires healthcare organizations to employ standardized electronic transactions, codes, and identifiers to enable them to fully digitize medical records, thus making it possible to exchange medical data over the Internet. The Department of Health and Human Services developed over 1,500 pages of specific rules governing exchange of such data. At the time of their implementation, these regulations affected more than 1.5 million healthcare providers, 7,000 hospitals, and 2,000 healthcare plans.[12] The rules, codes, and formats for exchanging digital medical records continue to change, making for an ongoing maintenance and training workload for the individuals and organizations involved.

Under the HIPAA provisions, healthcare providers must obtain written consent from patients prior to disclosing any information from their medical records. Thus, patients need to sign a HIPAA disclosure form each time they are treated at a hospital, and such a form must be kept on file with their primary care physician. In addition, healthcare providers are required to keep track of everyone who receives information from a patient's medical file.

For their part, healthcare companies must appoint a privacy officer to develop privacy policies and procedures as well as train employees on how to handle sensitive patient data. These actions must address the potential for unauthorized access to data by outside hackers as well as the more likely threat of internal misuse of data.

The penalties for noncompliance are based on the level of negligence, and violations can also carry criminal charges that can result in jail time. New York and Presbyterian Hospital and Columbia University agreed to pay $4.8 million to settle charges that they potentially violated HIPAA regulations by failing to secure thousands of patients' electronic protected health information held on their network.[13]

HIPAA assigns responsibility to healthcare organizations, as the originators of individual medical data, for certifying that their business partners (billing agents, insurers, debt collectors, research firms, government agencies, and charitable organizations) also comply with HIPAA security and privacy rules. This provision of HIPAA is of particular concern for many healthcare executives, as they do not have direct control over the systems and procedures that their partners implement.

The U.S. Department of Health and Human Services' Office for Civil Rights (OCR) is a federal agency responsible for enforcing civil rights and health-privacy rights. Following a complaint investigation or a compliance review, OCR sometimes determines that it is necessary to negotiate resolution agreements to force organizations to revise their policies, practices, and procedures to comply with federal civil rights laws including HIPAA.[14]

Some medical personnel and privacy advocates fear that between the increasing demands for disclosure of patient information and the inevitable complete digitization of medical records, patient confidentiality will be lost. Many think that HIPAA provisions are too complicated and that, rather than achieving the original objective of reducing medical industry costs, HIPAA has increased costs and paperwork for doctors without improving medical care. In addition, the Executive Leadership Group of Vice Presidents for Research of the Association of Academic Health Centers (AAHC) has concluded that the myriad regulations and mandates associated with HIPAA has raised unintended barriers that hamper medical research processes and progress.[15] All agree that the medical industry has had to make a substantial investment to achieve compliance.

The American Recovery and Reinvestment Act (2009)

The **American Recovery and Reinvestment Act** (Public Law 111-5) is a wide-ranging act passed in 2009 that authorized $787 billion in spending and tax cuts over a 10-year period. Title XIII, Subtitle D, of this act (known as the Health Information Technology for Economic and Clinical Health Act, or HITECH) included strong privacy provisions for electronic health records (EHRs), including banning the sale of health information, promoting the use of audit trails and encryption, and providing rights of access for patients. It also mandated that each individual whose health information has been exposed be notified within 60 days after discovery of a data breach.

Children's Personal Data

A recent survey revealed that teens spend more than nine hours per day on average watching television, playing video games, social networking, browsing websites, or doing other things on a computer, smartphone, or tablet.[16] Tweens (children aged 8 to 12) spend about six hours on average consuming media. Many people feel that there is a need to protect children from being exposed to inappropriate material and online predators; becoming the target of harassment; divulging personal data; and becoming involved in gambling or other inappropriate behavior. To date, only a few laws have been implemented to protect children online, and most of these have been ruled unconstitutional under the First Amendment and its protection of freedom of expression.

Family Educational Rights and Privacy Act (1974)

The **Family Educational Rights and Privacy Act (FERPA)** (20 U.S.C. § 1232g) is a federal law that assigns certain rights to parents regarding their children's educational records. These rights transfer to the student once the student reaches the age of 18, or earlier, if he or she attends a school beyond the high school level. These rights include:

- the right to access educational records maintained by a school;
- the right to demand that educational records be disclosed only with student consent;
- the right to amend educational records; and
- the right to file complaints against a school for disclosing educational records in violation of FERPA.

Under FERPA, the presumption is that a student's records are private and not available to the public without the consent of the student. Penalties for violation of FERPA may include a cutoff of federal funding to the educational institution. Educational agencies and institutions *may* disclose education records to the parents of a dependent student, as defined in Section 152 of the Internal Revenue Code of 1986, without the student's consent.

FERPA was implemented before the birth of the Internet and the widespread use of databases at various agencies, institutions, and organizations that attempt to service young people. The stringent restrictions of FERPA have frustrated attempts by such groups to share data about young people in common sense ways and have caused duplication of efforts and recordkeeping. New regulations issued by the U.S. Department of Education in late 2011 loosened the restrictions on sharing such data. Among other changes, state and local education authorities can now share data with other government agencies, as long as those other agencies are involved in federal or state-supported education programs.[17]

Children's Online Privacy Protection Act (1998)

According to the **Children's Online Privacy Protection Act (COPPA)** (15 U.S.C. §§ 6501–6506), any website that caters to children must offer comprehensive privacy policies, notify parents or guardians about its data collection practices, and receive parental consent before collecting any personal information from children under 13 years of age. COPPA was implemented in 1998 in an attempt to give parents control over the collection, use, and disclosure of their children's personal information; it does not cover the dissemination of information to children.

The law has had a major impact and has required many companies to spend hundreds of thousands of dollars to make their sites compliant; other companies eliminated preteens as a target audience.

Hasbro, Mattel, Viacom, and JumpStart Games were fined a total of $835,000 in 2016 for violation of the COPPA in connection with technology used by these companies that allowed third-party marketing and advertising companies to use cookies and IP addresses to gain access to the personal information of children under 13 years old without getting their parents' approval first. The companies were also forced to change their systems to protect the information of child users from being tracked.[18,19]

Electronic Surveillance

This section discusses government surveillance, including various forms of electronic surveillance, as well as some of the laws governing those activities. In recent years, new laws addressing government surveillance have been added and old laws amended in reaction to the development of new communication technologies and a heightened awareness of potential terrorist threats against Americans at home and abroad. The net result is that the scope of government surveillance has greatly expanded—going from collecting data on as few people as necessary to collecting data on as many people as possible.

Many of the resulting surveillance activities are viewed by some as an unconstitutional violation of the Fourth Amendment, which protects us from illegal searches and seizures. As a result, there are frequent court challenges to these government actions, as well as an ongoing public debate about whether such activities make us Americans safer or simply erode our rights to privacy.

Some people also feel that our basic rights of freedom of expression and association are violated when the U.S. government conducts widespread electronic surveillance on U.S. citizens. For instance, some people who belong to particular ethnic, religious, and social groups (including political activists on both ends of the political spectrum) are concerned that private data collected by the government could at some point be used to identify and target them and their associates. There is also concern that our past communications may be used in the future to implicate us in crimes that were once private and innocent acts. On the other hand, many Americans feel that the U.S. government is obligated to do all that it can do to provide for the security of its citizens, even it means violating some of the rights designed to protect our privacy. After all, they argue, if you are not doing anything "wrong," you should have no concerns.

Figure 4-2 provides a timeline for the enactment of some of the most significant laws and executive orders addressing issues of governmental surveillance.

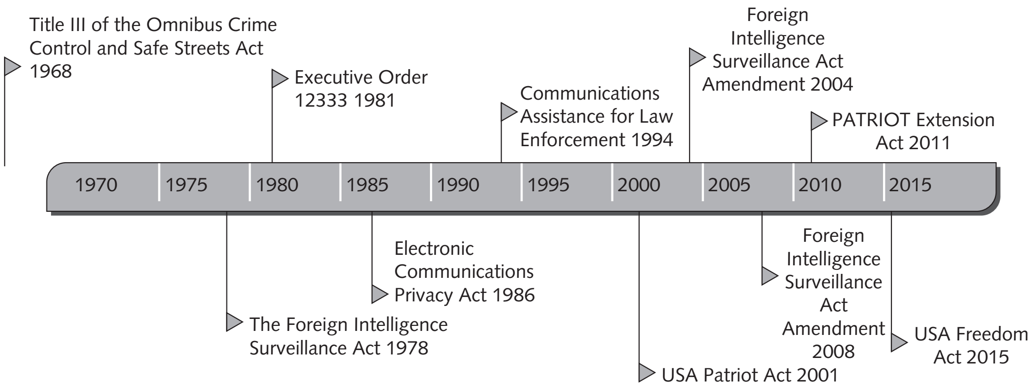

Title III of the Omnibus Crime Control and Safe Streets Act 1968
Executive Order 12333 1981
Communications Assistance for Law Enforcement 1994
Foreign Intelligence Surveillance Act Amendment 2004
PATRIOT Extension Act 2011
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
The Foreign Intelligence Surveillance Act 1978
Electronic Communications Privacy Act 1986
USA Patriot Act 2001
Foreign Intelligence Surveillance Act Amendment 2008
USA Freedom Act 2015

FIGURE 4-2 Various laws affecting electronic surveillance

Title III of the Omnibus Crime Control and Safe Streets Act (1968; amended 1986)

Title III of the Omnibus Crime Control and Safe Streets Act (Public Law 90-351), also known as the **Wiretap Act**, regulates the interception of wire (telephone) and oral communications. It allows state and federal law enforcement officials to use wiretapping and electronic eavesdropping, but only under strict limitations. Under this act, a warrant must be obtained from a judge to conduct a wiretap. The judge may approve the warrant only if "there is probable cause [to believe] that an individual is committing, has committed, or is about to commit a particular offense … [and that] normal investigative procedures have been tried and have failed or reasonably appear to be unlikely if tried or to be too dangerous."[20]

One of the driving forces behind the passage of this act was the case of *Katz v. United States*. Katz was convicted of illegal gambling based on recordings by the FBI of Katz's side of various telephone calls made from a public phone booth; the recordings were made using a device attached to the phone booth. Katz challenged the conviction based on a violation of his Fourth Amendment rights. In 1967, the case finally made it to the Supreme Court, which agreed with Katz. The Court ruled that "the Government's activities in electronically listening to and recording the petitioner's words violate the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[21] This ruling helped form the basis for the requirement that there be a reasonable expectation of privacy for the Fourth Amendment to apply.

Title III court orders must describe the duration and scope of the surveillance, the conversations that may be captured, and the efforts to be taken to avoid capture of innocent conversations. A total of 4,148 wiretaps were authorized in 2015, with 1,403 authorized by federal judges and 2,745 authorized by state judges. The most frequently noted location in wiretap applications was a "portable device" (96 percent of the time). This category includes cell phone communications, text messages, and software apps. In 2015, for reported intercepts, installed wiretaps were in operation for an average of 43 days. The federal wiretap with the most intercepts occurred during a narcotics investigation in the district of South Carolina and resulted in the interception of 81,122 messages over 300 days, including 35,402 incriminating interceptions.[22] These numbers include numbers from only reporting 25 states, and do not include wiretap orders in terrorism investigations, which are authorized by the Foreign Intelligence Surveillance Act (FISA) Court.

Since the Wiretap Act was passed, it has been significantly amended by several new laws, including FISA, ECPA, CALEA, and the USA PATRIOT Act—all of which are discussed later in this section.

The Foreign Intelligence Surveillance Act (1978)

The **Foreign Intelligence Surveillance Act (FISA)** (50 U.S.C.) describes procedures for the electronic surveillance and collection of foreign intelligence information in communications between foreign powers and the agents of foreign powers. **Foreign intelligence** is information relating to the capabilities, intentions, or activities of foreign governments or agents of foreign governments or foreign organizations. The act allows surveillance, without court order, within the United States for up to a year unless the "surveillance will acquire the contents of any communication to which a U.S. person is a party."[23] If a U.S. citizen is involved, judicial authorization is required within 72 hours after surveillance begins. The act also specifies that the U.S. attorney general may request a specific communications common carrier (a company that provides communications transmission services to the public) to furnish information, facilities, or technical assistance to accomplish the electronic surveillance.

FISA requires the government to obtain an individualized court order before it can intentionally target a U.S. person anywhere in the world to collect the content of his/her communications. Under FISA, a **U.S. person** is defined as a U.S. citizen, permanent resident, or company. The FISA court must be satisfied, based on a probable cause standard, that the U.S. person is an agent of a foreign power or an officer or employee of a foreign power.

FISA also created the **FISA Court**, which meets in secret to hear applications for orders approving electronic surveillance anywhere within the United States. Each application for a surveillance warrant is made before an individual judge of the court. Such applications are rarely turned down, as shown in Figure 4-3. Between 2001 and 2015, more than 25,000 applications were submitted to the FISA court, and only 12 of those were rejected.[24]

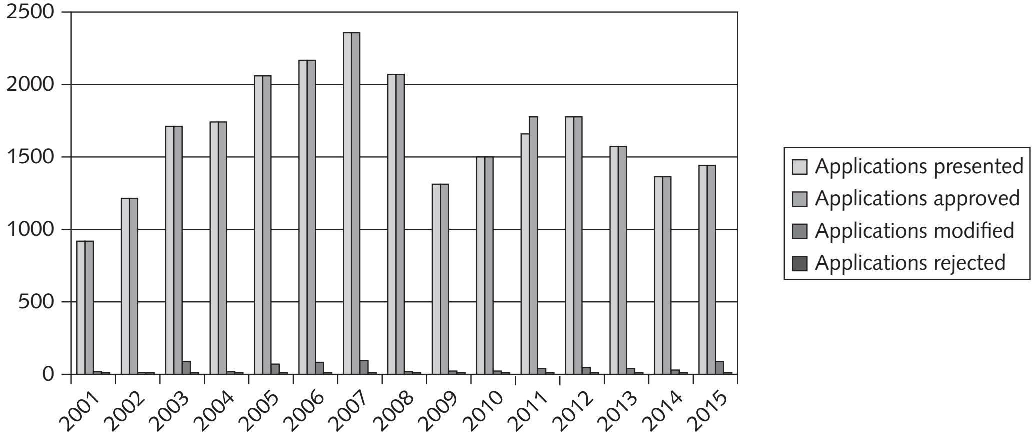


FIGURE 4-3 FISA court applications are almost never modified or rejected

Source: "Foreign Intelligence Surveillance Act Court Orders 1979-2015," Electronic Privacy Information Center, https://epic.org/privacy/surveillance/fisa/stats/default.html, accessed November 23, 2016.

Executive Order 12333 (1981)

An executive order is an official document used by the president of the United States to manage the operations of the federal government. Executive orders are subject to judicial review, and may be struck down if considered by the courts to be unsupported by statute or the Constitution. Many executive orders pertain to routine administrative matters and the internal operations of federal agencies. However, some executive orders have a much more visible impact. For instance, in 1863, President Lincoln issued the Emancipation Proclamation, an executive order, to free all persons held as slaves in the United States, and in 1942, President Roosevelt issued an executive order to intern Japanese-Americans in prison camps.

Executive Order 12333, which was issued by President Reagan in 1981 and has been amended several times, identifies the various U.S. governmental intelligence-gathering agencies (see Table 4-2) and defines what information can be collected, retained, and disseminated by these agencies. Under Executive Order 12333, intelligence-gathering agencies are allowed to collect information—including message content—obtained in the course of a lawful foreign intelligence, counterintelligence, international drug, or international terrorism investigation, as well as incidentally obtained information that may indicate involvement in activities that may violate federal, state, local, or foreign laws. This tangential collection of U.S. citizen data—even when those citizens are not specifically targeted—is forbidden under FISA. Thus, there is an unresolved conflict between Executive Order 12333 and FISA.

TABLE 4-2 Intelligence-gathering units of the U.S. government defined in executive order 12333

Central Intelligence Agency	Defense Intelligence Agency	National Security Agency
National Reconnaissance Office	National Geospatial-Intelligence Agency	Intelligence and Counterintelligence elements of the Army, Navy, Air Force, Marine Corps, and Coast Guard
Federal Bureau of Investigation	Bureau of Intelligence and Research	Department of State
Office of Intelligence and Analysis	Department of Treasury	Office of National Security Intelligence
Drug Enforcement Administration	Department of Homeland Security	Office of Intelligence and Counterintelligence
Department of Energy	Office of the Director of National Intelligence	

Executive Order 12333 also approves the use of any intelligence collection techniques that are in accordance with procedures established by the head of the intelligence community and approved by the attorney general. There is limited congressional review and oversight of these procedures, and they have never been publicly debated or voted on by Congress.

Electronic Communications Privacy Act (1986)

The **Electronic Communications Privacy Act (ECPA)** (18 U.S.C. § 2510-22) deals with three main issues: (1) the protection of communications while in transfer from sender to receiver; (2) the protection of communications held in electronic storage; and (3) the prohibition of devices from recording dialing, routing, addressing, and signaling information without a search warrant. ECPA was passed as an amendment to Title III of the Omnibus Crime Control and Safe Streets Act.

Title I of ECPA extends the protections offered under the Wiretap Act to electronic communications, such as email, fax, and text messages sent over the Internet. The government is prohibited from intercepting such messages unless it obtains a court order based on probable cause (the same restriction that is in the Wiretap Act relating to telephone calls).

Title II of ECPA (also called the Stored Communications Act) prohibits unauthorized access to stored wire and electronic communications, such as the contents of email inboxes, text messages, message boards, and social networking sites. However, the law only applies if the stored communications are not readily accessible to the general public. Webmasters who desire protection for their subscribers under this act must take careful measures to limit public access through the use of logon procedures, passwords, and other methods. Under this act, the FBI director or someone acting on his behalf may issue a **National Security Letter (NSL)** to an Internet service provider to provide various data and records about a service subscriber. An NSL compels holders of your personal records to turn them over to the government; an NSL is not subject to judicial review or oversight. Figure 4-4 shows the number of NSLs issued for the time period 2005 to 2015.

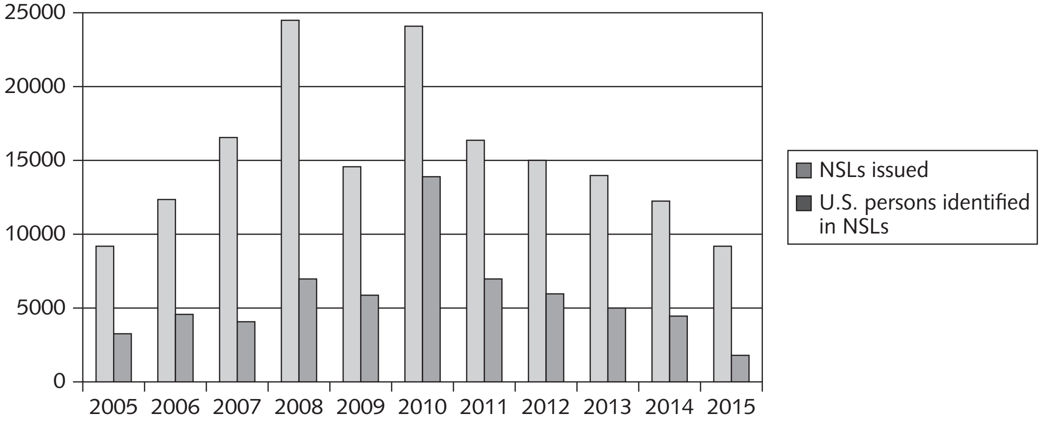


FIGURE 4-4 National Security Letters issued between 2005 and 2015

Source: "Foreign Intelligence Surveillance Act Court Orders 1979-2015," Electronic Privacy Information Center, https://epic.org/privacy/surveillance/fisa/stats/default.html, accessed November 23, 2016.

The third part of ECPA establishes a requirement for court-approved law enforcement use of a **pen register**—a device that records electronic impulses to identify the numbers dialed for outgoing calls—or a **trap and trace**—a device that records the originating number of incoming calls for a particular phone number. A recording of every telephone number dialed and the source of every call received can provide an excellent profile of a person's associations, habits, contacts, interests, and activities. A similar type of surveillance has also been applied to email communications to gather email addresses, email header information, and Internet provider addresses. To obtain approval for a pen-register order or a trap-and-trace order, the law enforcement agency only needs to certify that "the information likely to be obtained is relevant to an ongoing criminal investigation." (This requirement is much lower than the probable cause required to obtain a court order to intercept an electronic communication.) A prosecutor does not have to justify the request, and judges are required to approve every request.

Currently, there is no federal law that requires wireless carriers to save text messages sent by U.S. citizens. Congress is considering amending the ECPA to specify how long text messages must be stored and exactly what data about each text message must be stored (e.g., full text or simply identification of the sender, receiver, data, and time).[25]

Communications Assistance for Law Enforcement Act (1994)

The **Communications Assistance for Law Enforcement Act (CALEA)** (47 U.S.C. 1001-1010) was passed by Congress in 1994 and amended both the Wiretap Act and ECPA. CALEA was a hotly debated law because it required the telecommunications industry to build tools into its products that federal investigators could use—after obtaining a court order—to eavesdrop on conversations and intercept electronic communications. Such a court order can only be obtained if it is shown that a crime is being committed, that communications about the crime will be intercepted, and that the equipment being tapped is being used by the suspect in connection with the crime.[26]

A provision in the act covering radio-based data communication grew from a realization that the ECPA failed to cover emerging technologies, such as wireless modems, radio-based electronic mail, and cellular data networks. The ECPA statute outlawed the unauthorized interception of wire-based digital traffic on commercial networks, but the law's drafters did not foresee the growing interest in wireless data networks. Section 203 of CALEA corrected that oversight by effectively covering all publicly available "electronic communication."

With CALEA, the Federal Communications Commission responded to appeals from the Department of Justice and other law enforcement officials by requiring providers of Internet phone services and broadband services to ensure that their equipment accommodated the use of law enforcement wiretaps. This equipment includes Voice over Internet Protocol (VoIP) technology, which shifts calls away from the traditional phone network of wires and switches to technology based on converting sounds into data and transmitting them over the Internet. The decision has created a controversy among many who fear that opening VoIP to access by law enforcement agencies will create additional points of attack and security holes that hackers can exploit.

USA PATRIOT Act (2001)

The **USA PATRIOT Act** (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) (Public Law 107-56) was passed just five weeks after the terrorist attacks of September 11, 2001. It gave sweeping new powers to both domestic law enforcement and U.S. international intelligence agencies, including increasing the ability of law enforcement agencies to search telephone, email, medical, financial, and other records. It also eased restrictions on foreign intelligence gathering in the United States.

Although the act was more than 340 pages long and quite complex (it changed more than 15 existing statutes), it was passed into law just five weeks after being introduced. Legislators rushed to get the act approved in the House and Senate, arguing that law enforcement authorities needed more power to help track down terrorists and prevent future attacks. Critics have argued that the law removed many checks and balances that previously gave courts the opportunity to ensure that law enforcement agencies did not abuse their powers. Critics also argue that many of its provisions have nothing to do with fighting terrorism.

One of the more contentious aspects of the USA PATRIOT Act has been the guidelines issued for the use of NSLs. Before the USA PATRIOT Act was enacted, the FBI could issue an NSL to obtain information about someone only if it had reason to believe the person was a foreign spy. Under the USA PATRIOT Act, the FBI can issue an NSL to compel banks, Internet service providers, and credit reporting companies to turn over information about their customers without a court order simply on the basis that the information is needed for an ongoing investigation. The American Civil Liberties Union (ACLU) has challenged the use of NSLs by the FBI in court several times. These lawsuits are in various stages of hearings and appeals. In one lawsuit, *Doe v. Holder*, the Court of the Southern District of New York and, upon appeal, the Second Circuit Court of Appeals ruled that the **NSL gag provision**—which prohibits NSL recipients from informing anyone, even the person who is the subject of the NSL request, that the government has secretly requested his or her records—violates the First Amendment.[27]

The USA Freedom Act included modifications to the NSL provisions in the USA PATRIOT Act. Based on those changes, a district court has found NSLs to be constitutional. Under the old NSL provisions, courts were limited in being able to review NSLs. However, under the USA Freedom Act, there is at least some potential for judicial review, and that now makes them constitutional in the eyes of the court.[28]

Foreign Intelligence Surveillance Act Amendments Act (2004)

In 2004, Congress amended the FISA to authorize intelligence gathering on individuals not affiliated with any known terrorist organization (so-called lone wolves), with a sunset date to correspond with certain key provisions of the USA PATRIOT Act.

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008

A few months after the September 11, 2001, terrorist attacks, President George W. Bush signed an executive order that secretly authorized the NSA to monitor the international calls and emails of people inside the United States without court-approved warrants. The *New York Times* revealed the warrantless eavesdropping program in late 2005 after an investigation that lasted over a year. (Due to the controversial nature of the program, it was suspended temporarily in January 2007.) The Bush administration and other advocates of the program say this action was necessary to disrupt terrorist plots and prevent further attacks within the United States. Under this program, the NSA began warrantless eavesdropping on people in the United States who were linked to names and phone numbers found in terrorists' computers, cell phones, and rolodexes seized in various CIA operations overseas. Warrants were still required for eavesdropping on strictly domestic communications, say, phone calls from someone in Atlanta to a person in Los Angeles.[29] The disclosure of this secret program triggered three years of heated congressional debate that ended with Congress passing the **Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008**, granting NSA expanded authority to collect, *without court-approved warrants*, international communications as they flow through U.S. telecommunications network equipment and facilities. The targets of the warrantless eavesdropping had to be "reasonably believed" to be outside the United States; warrants were still required to monitor wholly domestic communications. The act also granted retroactive immunity from federal or civil action to any telecom firm that had participated in the warrantless eavesdropping program during the period of time this program could potentially be ruled illegal (September 2001 to January 2007).[30]

In 2009, the NSA notified members of various congressional intelligence committees that technical difficulties in distinguishing between wholly domestic and overseas communications had resulted in the collection of domestic communications without the required warrants.[31] The USA Freedom Act terminated the bulk collection of telephone metadata by the NSA in 2015.

PATRIOT Sunsets Extension Act of 2011

The **PATRIOT Sunsets Extension Act of 2011** (Public Law 112-14) granted a four-year extension of two key provisions in the USA PATRIOT Act that allowed roving wiretaps and searches of business records. This act also extended the 2004 FISA amendment that authorized intelligence gathering on "lone wolves." All three provisions are considered extremely useful by law enforcement officials but are opposed by some who say they can lead to privacy right abuses. These extensions were briefly allowed to expire in 2015 before being reinstated by the USA Freedom Act.

USA Freedom Act (2015)

The **USA Freedom Act** was passed following startling revelations by Edward Snowden (a former government contractor who copied and leaked classified information from the NSA in 2013 without authorization) of secret NSA surveillance programs. Here is a partial list of those revelations:[32,33]

- U.S. phone companies had been providing the NSA with all of their customers records, not just metadata (when each call was made and to what number).
- The NSA had been spying on over 120 world leaders, including German chancellor Angela Merkel, a U.S. ally.
- The NSA has developed a variety of tools to circumvent widely used Internet data encryption methods.
- An NSA team of expert hackers called the Tailored Access Operations hack into computers worldwide to infect them with malware.
- The FISA Court reprimanded the NSA for frequently providing misleading information about its surveillance practices.

The USA Freedom Act terminated the bulk collection of telephone metadata by the NSA. Instead, telecommunications providers are now required to hold the data and respond to NSA queries on the data. The act also restored authorization for roving wiretaps, which allows surveillance of individuals even if they frequently change communications devices, and the tracking of lone wolf terrorists.

Fair Information Practices

Fair information practices is a term for a set of guidelines that govern the collection and use of personal data. Various organizations as well as countries have developed their own set of such guidelines and call them by different names. The overall goal of such guidelines is to stop the unlawful storage of personal data, eliminate the storage of inaccurate personal data, and prevent the abuse or unauthorized disclosure of such data. For some organizations and some countries, a key issue is the flow of personal data across national boundaries (**transborder data flow**). Fair information practices are important because they form the underlying basis for many national laws addressing data privacy and data protection issues. Europe has been more active in this area than the United States and most of the national laws addressing data privacy originate in Europe.

Organisation for Economic Co-operation and Development for the Protection of Privacy and Transborder Flows of Personal Data (1980)

The Organisation for Economic Co-operation and Development (OECD) is an international organization currently consisting of 35 member countries, including Australia, Canada, France, Germany, Italy, Japan, Mexico, New Zealand, Turkey, the United Kingdom, and the United States. Its goals are to set policy and to come to agreement on topics for which multilateral consensus is necessary in order for individual countries to make progress in a global economy. Dialogue, consensus, and peer pressure are essential to make these policies and agreements stick.[34]

The OECD's fair information practices, established in 1980, are often held up as the model for ethical treatment of consumer data. These guidelines are composed of the eight principles summarized in Table 4-3. The OECD guidelines were nonbinding and as a result data privacy laws still vary widely across its member countries.[35]

TABLE 4-3 Summary of the 1980 OECD privacy guidelines

Principle	Guideline
Collection limitation	The collection of personal data must be limited; all such data must be obtained lawfully and fairly with the subject's consent and knowledge.
Data quality	Personal data should be accurate, complete, current, and relevant to the purpose for which it is used.
Purpose specification	The purpose for which personal data are collected should be specified and should not be changed.
Use limitation	Personal data should not be used beyond the specified purpose without a person's consent or by authority of law.
Security safeguards	Personal data should be protected against unauthorized access, modification, or disclosure.
Openness principle	Data policies should exist, and a data controller should be identified.
Individual participation	People should have the right to review their data, to challenge its correctness, and to have incorrect data changed.
Accountability	A data controller should be responsible for ensuring that the above principles are met.

Source: Organisation for Economic Co-operation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

European Union Data Protection Directive (1995)

The **European Union Data Protection Directive** (officially known as Directive 95/46/EC) requires any company doing business within the borders of the countries comprising the European Union (EU) to implement a set of privacy directives on the fair and appropriate use of information. Basically, this directive requires member countries to ensure that data transferred to non-EU countries is protected. It also bars the export of data to countries that do not have data privacy protection standards comparable to those of the EU. For example, in 2012, the European Commission approved New Zealand as a country that provides "adequate protection" of personal data under the directive so that personal information from Europe may flow freely to New Zealand.[36]

The following list summarizes the basic tenets of the directive:

- *Notice*—An individual has the right to know if his or her personal data are being collected, and any data must be collected for clearly stated, legitimate purposes.
- *Choice*—An individual has the right to elect not to have his or her personal data collected.
- *Use*—An individual has the right to know how personal data will be used and the right to restrict their use.
- *Security*—Organizations must "implement appropriate technical and organizations measures" to protect personal data, and the individual has the right to know what these measures are.
- *Correction*—An individual has the right to challenge the accuracy of the data and to provide corrected data.
- *Enforcement*—An individual has the right to seek legal relief through appropriate channels to protect privacy rights.[37]

Initially, EU countries were concerned that the largely voluntary system of data privacy in the United States did not meet the EU directive's stringent standards. Eventually, the U.S. Department of Commerce worked out an agreement with the EU; only U.S. companies that were certified as meeting certain "safe harbor" principles were allowed to process and store data of European consumers and companies. Thousands of U.S. multinational companies—such as Caterpillar, Experian, Ford, Gap Inc., Procter & Gamble, Pepsi, and Sony Music Entertainment—that need to exchange employee and consumer data among their subsidiaries to effectively operate their businesses have been certified. In addition, companies such as Facebook, Google, IBM, and Microsoft that provide email, social networking, or cloud computing services involving employee and consumer data have also been certified.[38]

In October 2015, however, the European Court of Justice declared invalid the Safe Harbor agreement between the EU and the United States that allowed some 4,400 organizations to transfer data in huge quantities to their servers in the United States.[39] The court took this action out of concern over "mass indiscriminate surveillance and interception" of personal data by the U.S. authorities—a direct result of revelations made by whistle-blower and former NSA contractor Edward Snowden. Because of this decision, the Safe Harbor framework has been replaced by the European–United States Privacy Shield Data Transfer Program.

European–United States Privacy Shield Data Transfer Program Guidelines

This new arrangement places stronger obligations on companies in the United States to protect the personal data of Europeans and requires stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission. Under this new arrangement, access to personal data by public authorities will be subject to clear conditions, limitations and oversight, preventing generalized access. To join the Privacy Shield Framework, a U.S.-based company will be required to self-certify to the Department of Commerce and publicly commit to comply with the Framework's requirements. While joining the Privacy Shield Framework will be voluntary, once an eligible company makes the public commitment to comply with the Framework's requirements, the commitment will become enforceable under U.S. law.[40]

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR; officially known as Regulation EU 2016/679) is designed to strengthen data protection for individuals within the EU by addressing the export of personal data outside the EU, enabling citizens to see and correct their personal data, and ensure data protection consistency across the EU. Organizations anywhere in the world that collect, store, or transfer personal data of EU citizens must work to ensure that their systems and procedures are compliant with this strict new framework. Noncompliance can result in penalties for privacy violations amounting to as much as four percent of a company's annual global revenue.[41]

When the GDPR takes effect in May 2018, it will repeal European Union Data Protection Directive (officially Directive 95/46/EC), the current data protection directive. That directive simply outlined recommendations and had no real enforcement requirements. This allowed the various EU countries to implement the recommendations as they saw fit, leading to significant differences from country to country. As a result, organizations operating in the EU have had to deal with a hodgepodge of data privacy laws governing the storing and processing of personal data. The GDPR regulation would simplify matters by enforcing a single set of rules for data protection across the EU. This will eliminate the need for costly administrative processes and save countries an estimated €2.3 billion (about $3.03 billion) per year.

The GDPR would also likely replace the Privacy Shield Framework. The GDPR rules are more comprehensive than the Privacy Shield rules and include the right to be forgotten, which requires organizations to delete the personal data of European citizens upon request.[42]

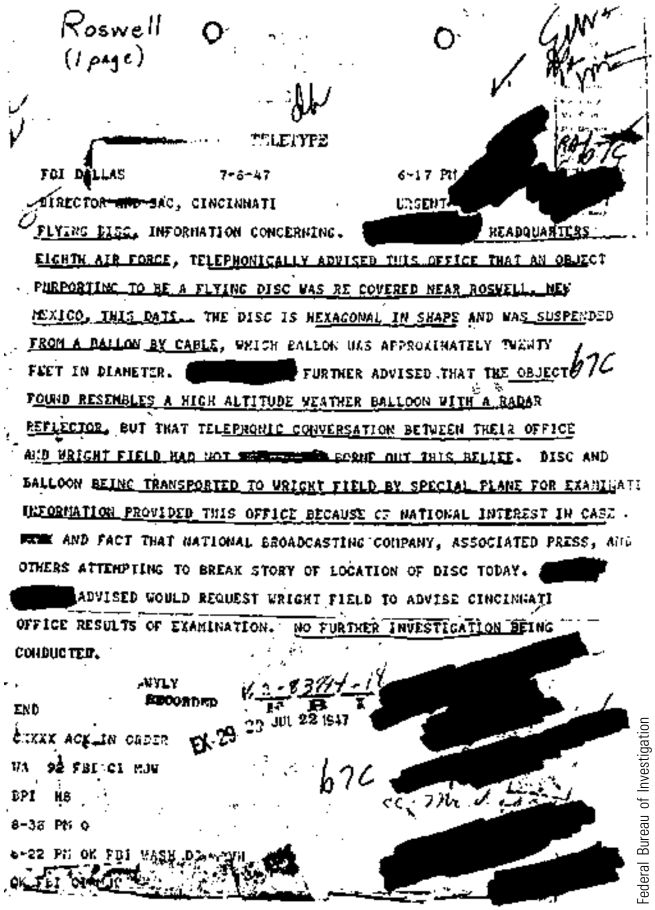
The United Kingdom's Tesco Bank was hit with a data breach in November 2016 that impacted some 40,000 customer accounts, with money taken from half of them.[43] Tesco Bank refunded £2.5 million ($3.2 million) to its current account customers following the attack. If the GDPR had been in effect at the time of the breach, Tesco Bank's parent company could have been facing a fine of nearly £2 billion ($2.5 billion).[44]

Access to Government Records

The U.S. government has a great capacity to store data about each and every one of us and about the proceedings of its various agencies. The Freedom of Information Act (FOIA) enables the public to gain access to certain government records, and the Privacy Act prohibits the government from concealing the existence of any personal data record-keeping systems.

Freedom of Information Act (1966; amended 1974)

The **Freedom of Information Act (FOIA)** grants citizens the right to access certain information and records of federal, state, and local governments upon request. FOIA is a powerful tool that enables journalists and the public to acquire information that the government is reluctant to release. The well-defined FOIA procedures have been used to uncover previously unrevealed details about President Kennedy's assassination, determine when and how many times members of Congress or certain lobbyists have visited the White House, obtain budget and spending data about a government agency, and even request information on the "UFO incident" at Roswell in 1947 (see Figure 4-5). Notice that much of the information in Figure 4-5 has been redacted, a practice common with FOIA requests.



Roswell
(1 page)

TELETYPE

FBI DALLAS 7-6-47 6-17 PM [redacted]

DIRECTOR ~~AND~~ SAC, CINCINNATI URGENT

FLYING DISC, INFORMATION CONCERNING. [redacted] HEADQUARTERS EIGHTH AIR FORCE, TELEPHONICALLY ADVISED THIS OFFICE THAT AN OBJECT PURPORTING TO BE A FLYING DISC WAS RE COVERED NEAR ROSWELL, NEW MEXICO, THIS DATE. THE DISC IS HEXAGONAL IN SHAPE AND WAS SUSPENDED FROM A BALLON BY CABLE, WHICH BALLON WAS APPROXIMATELY TWENTY FEET IN DIAMETER. [redacted] FURTHER ADVISED THAT THE OBJECT b7C FOUND RESEMBLES A HIGH ALTITUDE WEATHER BALLOON WITH A RADAR REFLECTOR, BUT THAT TELEPHONIC CONVERSATION BETWEEN THEIR OFFICE AND WRIGHT FIELD HAD NOT [redacted] BORNE OUT THIS BELIEF. DISC AND BALLOON BEING TRANSPORTED TO WRIGHT FIELD BY SPECIAL PLANE FOR EXAMINATI INFORMATION PROVIDED THIS OFFICE BECAUSE OF NATIONAL INTEREST IN CASE . [redacted] AND FACT THAT NATIONAL BROADCASTING COMPANY, ASSOCIATED PRESS, AND OTHERS ATTEMPTING TO BREAK STORY OF LOCATION OF DISC TODAY. [redacted] ADVISED WOULD REQUEST WRIGHT FIELD TO ADVISE CINCINNATI OFFICE RESULTS OF EXAMINATION. NO FURTHER INVESTIGATION BEING CONDUCTED.

ANVLY
RECORDED
62-83894-18
EX-29
23 JUL 22 1947

[redacted]

END

CXXXX ACK IN ORDER

WA 92 FBI CI MJW

DPI HS

8-38 PM O

6-22 PM OK FBI WASH DC

OK FBI CI

b7C

cc

FIGURE 4-5 Redacted response to FOIA request about Roswell incident

Federal Bureau of Investigation

The FOIA is often used by whistle-blowers to obtain records that they would otherwise be unable to get. Citizens have also used FOIA to find out what information the government has about them.

There are two basic requirements for filing a FOIA request: (1) the request must not require wide-ranging, unreasonable, or burdensome searches for records and (2) the request must be made according to agency procedural regulations published in the *Federal Register*. A typical FOIA request includes the requester's statement: "pursuant to the Freedom of Information Act, I hereby request"; a reasonably described record; and a statement of willingness to pay for reasonable processing charges. (The fees can be substantial and include the cost to search for the documents, the cost to review documents to see if they should be disclosed, and the cost of duplication.) FOIA requests are sent to the FOIA officer for the responding agency.[45]

Agencies receiving a request must acknowledge that the request has been received and indicate when the request will be fulfilled. The act requires an initial response within 20 working days unless an unusual circumstance occurs. In reality, most requests take much longer. The courts have ruled that this is acceptable as long as the agency treats each request sequentially on a first-come, first-served basis.

If a request filed under the FOIA is denied, the responding agency must provide the reasons for the denial along with the name and title of each denying officer. The agency must also notify the requester of his or her right to appeal the denial and provide the address to which an appeal should be sent. During 2015, the federal government processed a record high of 769,903 FOIA requests, with 37,860 requests (4.9 percent of the total filed) denied in full.[46]

An agency can deny a FOIA request based on the following nine document exemptions:[47]

1. Information properly classified as secret in the interest of national security
2. Information related solely to internal personnel rules and practices of an agency
3. Information that is prohibited from disclosure based on other federal statutes
4. Trade secrets or privileged or confidential commercial or financial information
5. Privileged communications within or between agencies
6. A personnel, medical, or similar file the release of which would constitute a clearly unwarranted invasion of personal privacy
7. Information compiled for law enforcement purposes, the release of which
   a. could reasonably be expected to interfere with law enforcement proceedings,
   b. would deprive a person of a right to a fair trial or an impartial adjudication,
   c. could reasonably be expected to constitute an unwarranted invasion of personal privacy,
   d. could reasonably be expected to disclose the identity of a confidential source,
   e. would disclose techniques, procedures, or guidelines for investigations or prosecutions, or
   f. could reasonably be expected to endanger an individual's life or physical safety.

8. Information that concerns the supervision of financial institutions
9. Documents containing exempt information about gas or oil wells

The use of the FOIA to access information can lead to a dispute between those who feel it is important certain information be revealed and those who feel certain government data should not be made public, including, in some cases, those whose privacy is being impacted.

Phil Eil has been attempting to write a book about the trial of Paul Volkman, a Chicago physician who was sentenced in 2012 to four consecutive life terms for illegally prescribing and distributing pain medications. Volkman's trial lasted eight weeks, and included 70 witnesses and over 220 exhibits.[48] Following the trial, the DEA has prevented everyone from viewing the evidence from the trial. Eil was denied access to court documents by the U.S. district court clerk, appellate court clerk, the prosecutor, and the judge who presided over the case. Eil filed a FOIA request with the Department of Justice in 2012 but still was refused access. The denied request resulted in a lawsuit, which was filed in March 2015. Finally, in 2016, a U.S. district court judge ruled that Eil's request to view trial materials used to convict Volkman was legal and reasonable despite the DEA's insistence that the release would compromise the privacy of numerous people, including trial witnesses.[49]

The government can respond in various ways to FOIA requests other than by providing access to the full and unadulterated documents requested. For example, the ACLU filed a FOIA request for information regarding the Justice Department's policy on intercepting text messages on cellphones. In response, the ACLU received a 15-page response in which every single page was redacted from top to bottom.[50] In 2014, journalist Victor Hugo Michel submitted a FOIA request for information about drug kingpin Joaquin "El Chapo" Guzman and was told that he would have to pay $1.46 million in fees to cover the cost of pulling information to meet his request.[51]

Privacy Act (1974)

The **Privacy Act** establishes a code of fair information practices that sets rules for the collection, maintenance, use, and dissemination of personal data that is kept in systems of records by federal agencies. It also prohibits U.S. government agencies from concealing the existence of any personal data record-keeping system. Under this law, any agency that maintains such a system must publicly describe both the kinds of information in it and the manner in which the information will be used. The law also outlines 12 requirements that each record-keeping agency must meet, including those that address issues such as openness, individual access, individual participation, collection limitation, use limitation, disclosure limitation, information management, and accountability. The purpose of the act is to provide safeguards for people against invasion of personal privacy by federal agencies. The CIA and law enforcement agencies are excluded from this act; in addition, it does not cover the actions of private industry.[52]

Several individuals and organizations have attempted unsuccessfully to sue various federal agencies for what they perceive to be violations of the Privacy Act. For instance, in 2004, miners sued the Department of Labor for disclosing their Social Security numbers in connection with the publication of their black lung compensation claims. The Supreme

Court ruled in a case involving one of those miners that an individual can file suit against the government to recover financial damages when personal information is exposed only if an "actual damage" is proven, which it deemed the miner had not proved. In 2011, the Department of Defense and Science Applications International Corporation (a provider of government services and information technology support) was sued under the Privacy Act after military health insurance data on 4.9 million service members and their families were stolen. In this case, a federal judge ruled that data loss alone, without evidence the information was misused, did not merit damages.[53] In another case from 2012, the Supreme Court decided that a Federal Aviation Administration employee whose HIV-positive condition was disclosed could not claim financial damages based on mental or emotional distress caused by a federal agency's intentional or willful violation of the Privacy Act.[54]

CRITICAL THINKING EXERCISE: HIPAA REGULATIONS RAISE CONCERN

HIPAA assigns responsibility to healthcare organizations, as the originators of individual medical data, for certifying that their business partners (billing agents, insurers, debt collectors, research firms, government agencies, and charitable organizations) also comply with HIPAA security and privacy rules. This provision of HIPAA has healthcare executives especially concerned, as they do not have direct control over the systems and procedures that their partners implement.

Which HIPAA provisions do you think cause the most concern? What measures might a healthcare organization take to ensure that its business partners are compliant with these provisions?

KEY PRIVACY AND ANONYMITY ISSUES

The rest of this chapter discusses a number of current and important privacy issues, including consumer profiling, electronic discovery, workplace monitoring, and advanced surveillance technology.

Consumer Profiling

Companies openly collect personal information about users when they register at websites, complete surveys, fill out forms, follow them on social media, or enter contests online. Many companies also obtain personal information through the use of **cookies**—text files that can be downloaded to the hard drives of users who visit a website, so that the website is able to identify visitors on subsequent visits. Companies also use tracking software to allow their websites to analyze browsing habits and deduce personal interests and preferences. The use of cookies and tracking software is controversial because companies can collect information about consumers without their explicit permission.

After cookies have been stored on your computer, they make it possible for a website to tailor the ads and promotions presented to you. The marketer knows what ads have been viewed most recently and makes sure that they aren't shown again, unless the advertiser has decided to market using repetition. Some types of cookies can also track what other sites a user has visited, allowing marketers to use that data to make educated guesses about the kinds of ads that would be most interesting to the user.

Offline, marketing firms employ similarly controversial means to collect information about people and their buying habits. Each time a consumer uses a credit card, redeems frequent flyer points, fills out a warranty card, answers a phone survey, buys groceries using a store loyalty card, or registers a car with the DMV (Department of Motor Vehicles), the data are added to a storehouse of personal information about that consumer, which may be sold or shared with third parties. In many of these cases, consumers never explicitly consent to submitting their information to a marketing organization.

Marketing firms aggregate the information they gather about consumers to build databases that contain a huge amount of consumer data. They want to know as much as possible about consumers—who they are, what they like, how they behave, and what motivates them to buy. The marketing firms provide these data to companies so that they can tailor their products and services to individual consumer preferences. Advertisers use the data to more effectively target and attract customers to their messages. Ideally, this means that buyers should be able to shop more efficiently and find products that are well suited for them. Sellers should be better able to tailor their products and services to meet their customers' desires and to increase sales. However, concerns about how these data are used prevent many potential online shoppers from making purchases.

Online marketers cannot capture personal information, such as names, addresses, and Social Security numbers, unless people provide them. Without this information, companies can't contact individuals who visit their websites. Data gathered about a user's web browsing through the use of cookies are anonymous, as long as the network advertiser doesn't link the data with personal information. However, if a visitor to a website volunteers personal information, a website operator can use it to find additional personal information that the visitor may not want to disclose. For example, a name and address can be used to find a corresponding phone number, which can then lead to obtaining even more personal data. All these information become extremely valuable to the website operator, who is trying to build a relationship with website visitors and turn them into customers. The operator can use these data to initiate contact or sell it to other organizations with which they have marketing agreements.

Opponents of consumer profiling are concerned that personal data are being gathered and sold to other companies without the permission of consumers who provide the data. After the data have been collected, consumers have no way of knowing how it is used or who is using it. In fact, consumer data privacy has grown into a major marketing issue.

Companies that can't protect or don't respect customer information often lose business, and some become defendants in class action lawsuits stemming from privacy violations. **A data breach** is the unintended release of sensitive data or the access of sensitive data (e.g., credit card numbers, health insurance member ids, and Social Security numbers) by unauthorized individuals. The cost to an organization that suffers a data breach can be quite high—by some estimates nearly $200 for each record lost. Nearly half the cost is typically a result of lost business opportunity associated with the customers whose patronage has been lost due to the incident. Other costs include public relations–related costs to manage the firm's reputation, and increased customer-support costs for information hotlines and credit monitoring services for victims. Table 4-4 lists the largest U.S. data breaches in the past five years.[55,56]

TABLE 4-4 Largest data breaches in the past five years

Organization	Year breach occurred	Number of records compromised	Data stolen
Yahoo	2013	1 billion	Usernames, passwords, email addresses, and security questions and answers
Yahoo	2014	500 million	Real names, dates of birth, email addresses, and telephone numbers
FriendFinder	2016	412 million	Usernames, passwords, and email addresses
LinkedIn	2012	165 million	Email addresses and passwords
Target	2013	110 million	Real names, addresses, email addresses, telephone numbers, and credit and debit card data

The 2013 data breach at Target affected 40 million debit and credit card accounts along with the personal information (names, phone numbers, and email and mailing addresses) of up to an additional 70 million customers.[57] Target reported that it incurred more than $248 million in costs connected to the data breach, an amount partially offset by an insurance payout of $90 million. Target's total costs include estimates for the costs the company expects to bear in the future, including liabilities to payment card networks for reimbursement of credit card fraud, liabilities from civil lawsuits, costs to reissue cards, investigative and consulting fees, and expenses and capital investments for remediation activities.[58] In addition, sales in the fourth quarter of the company's fiscal year 2013 (which ended February 1, 2014) fell $800 million from the year before—some portion of this is likely due to loss of customer goodwill caused by the data breach.[59] The cost to banks and credit unions for issuing replacement cards connected to the Target breach is estimated to exceed $200 million. Data to create some 1 to 3 million fraudulent cards were stolen and sold on the black market before the issuing banks could cancel them. Because consumers are not held responsible for fraudulent charges on their cards, there is an additional cost for fraudulent activity that could reach as high as $100 million.[60] These costs are summarized in Figure 4-6.

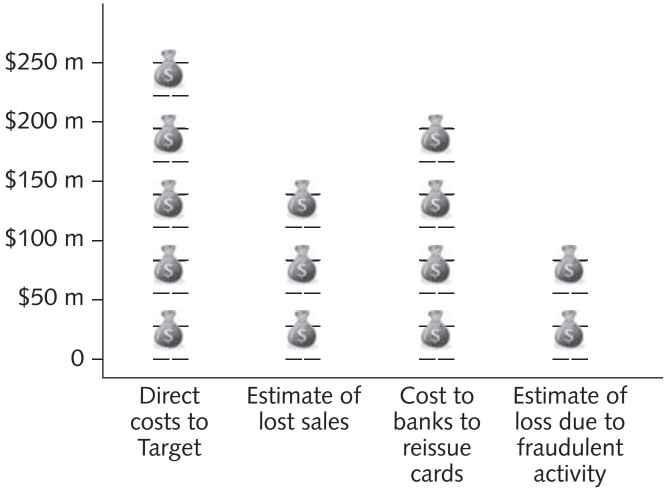


FIGURE 4-6 Costs associated with the 2013 Target data breach

Identity theft is the theft of personal information, which is then used without the owner's permission. Often, stolen personal identification information, such as a person's name, Social Security number, or credit card number, is used to commit fraud or other crimes. Thieves may use a consumer's credit card number to charge items to that person's account, use identification information to apply for a new credit card or a loan in a consumer's name, or use a consumer's name and Social Security number to obtain government benefits. Thieves also often sell personal identification information on the black market.[61] The Identity Theft and Assumption Deterrence Act (18 U.S.C. § 1028) makes identity theft a federal crime, with penalties of up to 15 years of imprisonment and a maximum fine of $250,000.

Organizations are often reluctant to announce data breaches due to the ensuing bad publicity and potential for lawsuits by angry customers. However, victims whose personal data were compromised during a data breach need to be informed so that they can take protective measures.

Publicly traded organizations have an obligation to report *significant* data breaches to the Security and Exchange Commission. From January 2010 to September 2016, there were 2,642 actual data breaches at publicly traded companies (according to Privacy Rights Clearinghouse, a consumer advocacy group), but only 95 of these incidents were reported to the Securities and Exchange Commission. Chief financial officers at many of these nonreporting organizations claim the breaches were not material, meaning they were not significant enough to influence an investor's decision to buy a company stock. The Securities and Exchange Commission has yet to bring a case against a company that failed to disclose a data breach, but officials have not ruled out doing so.[62]

Most states have laws that require businesses to notify the state and/or affected consumers in a timely fashion of data breaches that compromise more than a set amount of consumer data. About 300 publicly listed U.S. companies reported cybersecurity incidents to a state regulator or directly to affected consumers over the past six years, although not all were reported in a timely fashion.[63] For example, the New York attorney general imposed a fine of $50,000 for delays in the reporting of two data breaches involving some

70,000 credit card numbers and other personal data at the Trump Hotels chain. As part of the settlement, Trump Hotels was also required to undertake additional security measures, including conducting annual employee security training, performing regular software security testing, and ensuring that contracted service providers implement and maintain appropriate safeguards.[64]

Electronic Discovery

Discovery is part of the pretrial phase of a lawsuit in which each party can obtain evidence from the other party by various means, including requests for the production of documents. The purpose of discovery is to ensure that all parties go to trial with as much knowledge as possible. Under the rules of discovery, neither party is able to keep secrets from the other. Should a discovery request be objected to, the requesting party may file a motion to compel discovery with the court.

Electronic discovery (e-discovery) is the collection, preparation, review, and production of electronically stored information for use in criminal and civil actions and proceedings. **Electronically stored information (ESI)** includes any form of digital information, including emails, drawings, graphs, web pages, photographs, word-processing files, sound recordings, and databases stored on any form of magnetic storage device, including hard drives, CDs, and flash drives. Through the e-discovery process, it is quite likely that various forms of ESI of a private or personal nature (e.g., personal emails) will be disclosed.

The Federal Rules of Procedure define certain processes that must be followed by a party involved in a case in federal court. Under these rules, once a case is filed, the involved parties are required to meet and discuss various e-discovery issues, such as how to preserve discoverable data, how the data will be produced, agreement on the format in which the data will be provided, and whether production of certain ESI will lead to waiver of attorney–client privilege. A key issue is the scope of e-discovery (e.g., how many years of ESI will be requested and what topics and/or individuals need to be included in the e-discovery process).

Often organizations will send a **litigation hold notice** that informs its employees (or employees or officers of the opposing party) to save relevant data and to suspend data that might be due to be destroyed based on normal data-retention rules. Apple and Samsung were embroiled in a dispute involving alleged patent infringement, which led to an additional dispute over litigation hold notices. During the patent infringement litigation, the court cited Samsung for failing to circulate a comprehensive litigation hold instruction among its employees when it first anticipated litigation. According to the court, this failure resulted in the loss of emails from several key Samsung employees. Samsung then raised the same issue—Apple had neglected to implement a timely and comprehensive litigation hold to prevent broad destruction of pertinent email. A key learning from this case is that an organization should focus on its own ESI preservation and production efforts before it raises issues with its opponent's efforts.[65]

Collecting, preparing, and reviewing the tremendous volume of ESI kept by an organization can involve significant time and expense. E-discovery is further complicated because there are often multiple versions of information (such as various drafts) stored in many locations (such as the hard drives of the creator and anyone who reviewed the document, multiple company file servers, and backup tapes). As a result, e-discovery can become so expensive and time consuming that some cases are settled just to avoid the costs.[66]

Traditional software development firms as well as legal organizations have recognized the growing need for improved processes to speed up and reduce the costs associated with e-discovery. As a result, dozens of companies now offer e-discovery software that provides the ability to do the following:

- Analyze large volumes of ESI quickly to perform early case assessments
- Simplify and streamline data collection from across all relevant data sources in multiple data formats
- Cull large amounts of ESI to reduce the number of documents that must be processed and reviewed
- Identify all participants in an investigation to determine who knew what and when

Predictive coding is a process that couples human guidance with computer-driven concept searching in order to "train" document review software to recognize relevant documents within a document universe. It is used to reduce a large set of miscellaneous documents that may or may not be of interest to a much smaller set of documents (5 to 20 percent of the original set) that are pertinent to a legal case or FOIA inquiry. Predictive coding greatly accelerates the actual review process while also improving its accuracy and reducing the risk of missing key documents. Two key issues are raised with the use of predictive coding: (1) are attorneys still able to meet their legal obligations to conduct a reasonable search for pertinent documents using predictive coding and (2) how can counsel safeguard a client's attorney-client privilege if a privileged document is uncovered?[67]

E-discovery raises many ethical issues: Should an organization ever attempt to destroy or conceal incriminating evidence that could otherwise be revealed during discovery? To what degree must an organization be proactive and thorough in providing evidence sought through the discovery process? Should an organization attempt to bury incriminating evidence in a mountain of trivial, routine ESI?

Workplace Monitoring

Cyberloafing is defined as using the Internet for purposes unrelated to work such as posting to Facebook, sending personal emails or Instant messages, or shopping online. It is estimated that cyberloafing costs U.S. business as much as $85 billion a year. Some surveys reveal that the least productive workers cyberloaf more than 60 percent of their time at work.[68]

Many organizations have developed policies on the use of IT in the workplace in order to protect against employee's abuses that reduce worker productivity or that expose the employer to harassment lawsuits. For example, an employee may sue his or her employer for creating an environment conducive to sexual harassment if other employees are viewing pornography online while at work and the organization takes no measures to stop such viewing. (Email containing crude jokes and cartoons or messages that discriminate against others based on gender, race, sexual orientation, religion, or national origin can also spawn lawsuits.) By instituting and communicating a clear IT usage policy, a company can establish boundaries of acceptable behavior, which enable management to take action against violators.

The potential for decreased productivity and increased legal liabilities has led many employers to monitor workers to ensure that corporate IT usage policies are being followed. Almost 80 percent of major companies choose to record and review employee communications and activities on the job, including phone calls, email, and web surfing. Some are even videotaping employees on the job. In addition, some companies employ random drug testing and psychological testing. With few exceptions, these increasingly common (and many would say intrusive) practices are perfectly legal.

The Fourth Amendment to the Constitution protects citizens from unreasonable government searches and is often invoked to protect the privacy of government employees. *Public-sector* workers can appeal directly to the "reasonable expectation of privacy" standard established by the 1967 Supreme Court ruling in *Katz v. United States*.

However, the Fourth Amendment cannot be used to limit how a *private* employer treats its employees. As a result, public-sector employees have far greater privacy rights than those in private industry. Although private-sector employees can seek legal protection against an invasive employer under various state statutes, the degree of protection varies widely by state. Furthermore, state privacy statutes tend to favor employers over employees. For example, to successfully sue an organization for violation of their privacy rights, employees must prove that they were in a work environment in which they had a reasonable expectation of privacy. As a result, courts typically rule against employees who file privacy claims for being monitored while using company equipment. A private organization can defeat a privacy claim simply by proving that an employee had been given explicit notice that email, files, and Internet data held on company computers and transferred over company networks were not private and might be monitored.

Your employer may legally monitor your use of any employer-provided mobile phone or computing device including contact lists, call logs, email, location, photos, videos, and web browsing. Many employers permit their employees to use their own personal mobile phones or computing devices for work purposes in a policy called Bring Your Own Device (BYOD). Such a policy should spell out the degree to which use of such devices may be monitored.

Many companies encourage their employees to wear fitness trackers as part of an organizational fitness program. Devices from Apple, Fitbit, and others collect valuable data on employee's health and physical movement but can also open the door to numerous ethical and legal issues. For example, suppose a production floor worker's tracking device reveals the worker is less mobile and active than his peers. Can the employer use this data to justify firing the employee or moving him to another position? Should the employer investigate whether the data indicate the worker has a physical disability that requires the employer to make a reasonable accommodation? If the employer takes no action, can the employer be sued for failure to provide a reasonable accommodation in light of evidence the worker had a disability?

Society is still struggling to define the extent to which employers should be able to monitor the work-related activities of employees. On the one hand, employers want to be able to guarantee a work environment that is conducive to all workers, ensure a high level of worker productivity, and limit the costs of defending against privacy-violation lawsuits filed by disgruntled employees. On the other hand, privacy advocates want federal legislation that keeps employers from infringing on the privacy rights of employees. Such legislation would require prior notification to all employees of the existence and location of all electronic monitoring devices. Privacy advocates also want restrictions on the types of information collected and the extent to which an employer may use electronic monitoring. As a result, privacy bills are being introduced and debated at the state and federal levels. As the laws governing employee privacy and monitoring continue to evolve, business managers must stay informed in order to avoid enforcing outdated usage policies. Organizations with global operations face an even greater challenge because the legislative bodies of other countries also debate these issues.

Sapience Analytics offers software that tracks employee activities (e.g., email, texting, calls, analysis, data collection, online meetings, and management activities) and displays them in an app that is visible to both employees and their managers. The tasks are also separated into categories, such as sales or marketing, so that users can see what percentage of their time is spent on the designated core activities and categories for their position. An IT services company that implemented the software as a "mentoring" tool for its 5,000 employees reported a 90-minute daily increase per person in "core activities" (i.e., coding for a software developer rather than answering emails) after employees were made aware of their work patterns.[69]

Advanced Surveillance Technology

A number of advances in information technology—such as surveillance cameras and satellite-based systems that can pinpoint a person's physical location—provide amazing new data-gathering capabilities. However, these advances can also diminish individual privacy and complicate the issue of how much information should be captured about people's private lives.

Advocates of advanced surveillance technology argue that people have no legitimate expectation of privacy in a public place and thus Fourth Amendment privacy rights do not apply. Critics raise concerns about the use of surveillance to secretly store images of people, creating a new potential for abuse, such as intimidation of political dissenters or blackmail of people caught with the "wrong" person or in the "wrong" place. Critics also raise the possibility that such technology may not identify people accurately.

Camera Surveillance

Surveillance cameras are used in major cities around the world in an effort to deter crime and terrorist activities. Critics believe that such scrutiny is a violation of civil liberties and are concerned about the cost of the equipment and people required to monitor the video feeds. Surveillance camera supporters offer anecdotal data that suggest the cameras are effective in preventing crime and terrorism. They can provide examples in which cameras helped solve crimes by corroborating the testimony of witnesses and helping to trace suspects.

There are 5.9 million closed circuit TV cameras (CCTV) in operation throughout Great Britain—which amounts to 1 CCTV camera for every 10 people.[70] China, by way of comparison, has installed 100 million surveillance cameras, or 1 camera for every 14 citizens.[71] The two most closely monitored cities in the world include Beijing with

477,000 cameras and London with 422,000.[72] The Chicago Transit Authority (CTA) has installed more than 23,000 cameras in an attempt to reduce crime on its rail and bus system. According to the CTA, the cameras aided in the arrest of 250 criminals and helped reduce the overall crime rate on the CTA system by 25 percent from the previous year.[73]

The Domain Awareness system is a joint effort of the New York Police Department and Microsoft to combat terrorist activities and reduce the time required to respond to an incident. The system links together the city's 9,000 surveillance cameras and 600 radiation detectors as well as license plate readers and NYPD computer records, including 911 calls. The 40 million dollar system is sensitive enough to tell if a radiation detector was set off by actual radiation, a weapon, or a harmless medical isotope. It can also find where a suspect's car is located and track where it has been for the past few weeks. If a suspicious package is left somewhere, police will be able to look back in time and see who left it there.[74,75] At a press conference announcing the system, New York City mayor Michael Bloomberg dismissed concerns that the system would enable police to achieve "Big Brother" capabilities stating, "What you're seeing is what the private sector has used for a long time. If you walk around with a cell phone, the cell phone company knows where you are …We're not your mom and pop's police department anymore."[76,77]

Vehicle Event Data Recorders

A **vehicle event data recorder (EDR)** is a device that records vehicle and occupant data for a few seconds before, during, and after any vehicle crash that is severe enough to deploy the vehicle's air bags. Sensors located around the vehicle capture and record information about vehicle speed and acceleration; seat belt usage; air bag deployment; activation of any automatic collision notification system; and driver inputs such as brake, accelerator, and turn signal usage.[78] The EDR cannot capture any data that could identify the driver of the vehicle. Nor can it tell if the driver was operating the vehicle under the influence of drugs or alcohol.

The U.S. government does not require EDRs in passenger vehicles. Vehicle manufacturers voluntarily elect to install EDRs, and the capabilities of EDRs vary from manufacturer to manufacturer. If fact, most vehicle owners don't know whether or not their vehicle has an EDR. Beginning with model year 2011 vehicles, the National Highway Traffic Safety Administration (NHTSA) defined a minimum set of 15 data elements that must be captured for manufacturers who voluntarily install EDRs on their vehicles. These data can be downloaded from the EDR and be used for analysis.

One purpose of the EDR is to capture and record data that can be used by the manufacturer to make future changes to improve vehicle performance in the event of a crash. Another purpose is for use in a court of law to determine what happened during a vehicle accident.

State laws dictate who owns the EDR data, and these provisions vary from state to state. NHTSA must ask permission from the owner of a vehicle before downloading any data for government analysis. Courts can subpoena EDR data for use in court proceedings. There have been numerous cases in which EDR data have been ruled as admissible and reliable in court hearings, and there are cases in which such data have had a significant impact on the findings of the court.[79] For example, in *Howard v. Miami Twp, Fire Div,*171 Ohio App.3d

184, 2007-Ohio-1508, an accident reconstruction expert was able to use EDR data to determine that the driver was exceeding the speed limit at the time of a fatal accident.[80]

The fact that most cars now come equipped with an EDR and that the data from this device may be used as evidence in a court of law is not broadly known by the public. The future capabilities of EDRs and the extent of use of their data in court proceedings remain to be seen.

Stalking Apps

Technology has made it easy for a person to track the whereabouts of someone else at all times, without ever having to follow the person. Cell phone spy software called a **stalking app** can be loaded onto someone's cell phone or smartphone within minutes, making it possible for the user to perform location tracking, record calls, view every text message or picture sent or received, and record the URLs of any website visited on the phone. A built-in microphone can be activated remotely to use as a listening device even when the phone is turned off.[81] All information gathered from such apps can be sent to the user's email account to be accessed live or at a later time. Some of the most popular spy software includes Mobile Spy, ePhoneTracker, FlexiSPY, and Mobile Nanny.[82]

There is no law that prohibits a business from making an app whose primary purpose is to help one person track another, and anyone can purchase this type of software over the Internet. (Some users of such software have complained that they contracted malware when downloading stalker apps or that the app failed to work as advertised.) However, it is illegal to install the software on a phone without the permission of the phone owner. It is also illegal to listen to someone's phone calls without their knowledge and permission. However, these legal technicalities are not a deterrent for a determined stalker.

CRITICAL THINKING EXERCISE: MONITORING WORKER PRODUCTIVITY

You are employed in the human resources organization of a small manufacturing company that is implementing a new inventory control system to track the quantity and movement of all finished goods stored in its warehouse. Each time a forklift operator moves a case of product, he must first scan the product identifier on the case. The product information is captured, as is the date, time, and forklift operator identification number. These data are transmitted over a wireless network to the inventory control application, which then transmits information to the operator telling him where the product should be placed in the warehouse.

The warehouse manager is excited about using case-movement data to monitor worker productivity. He will be able to tell how many cases per shift each operator moves, and he plans to use these data to provide performance feedback that could result in pay bonuses or a range of disciplinary actions up to and including termination. What potential problems could arise from using the system in this manner, and what could be done to avoid those problems?

Summary

What is the right of privacy, and what is the basis for protecting personal privacy under the law?

- The right of privacy is “the right to be left alone—the most comprehensive of rights, and the right most valued by a free people.”
- Information privacy is the combination of communications privacy (the ability to communicate with others without those communications being monitored by other persons or organizations) and data privacy (the ability to limit access to one’s personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and its use).
- The use of information technology in business requires balancing the needs of those who use the information that is collected against the rights and desires of the people whose information is being used. A combination of approaches—new laws, technical solutions, and privacy policies—is required to balance the scales.
- The Fourth Amendment reads, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” The courts have ruled that without a reasonable expectation of privacy, there is no privacy right to protect.
- Today, in addition to protection from government intrusion, people want and need privacy protection from private industry. For many, the existing hodgepodge of privacy laws and practices fails to provide adequate protection and fuels a sense of distrust and skepticism, and concerns over identity theft.

What are some of the laws that provide protection for the privacy of personal data, and what are some of the associated ethical issues?

- Few laws provide privacy protection from private industry and there is no single, overarching national data privacy policy for the United States.
- The Fair Credit Reporting Act regulates operations of credit reporting bureaus.
- The Right to Financial Privacy Act protects the financial records of financial institution customers from unauthorized scrutiny by the federal government.
- The GLBA established mandatory guidelines for the collection and disclosure of personal financial information by financial institutions; requires financial institutions to document their data security plans; and encourages institutions to implement safeguards against pretexting.
- The Fair and Accurate Credit Transaction Act allows consumers to request and obtain a free credit report each year from each of the three consumer credit reporting agencies.
- The HIPAA defined numerous standards to improve the portability and continuity of health insurance coverage; reduce fraud, waste, and abuse in health insurance care and healthcare delivery; and simplify the administration of health insurance.
- The American Recovery and Reinvestment Act included strong privacy provisions for EHRs, including banning the sale of health information, promoting the use of audit trails and encryption, and providing rights of access for patients. It also mandated that each individual whose health information has been exposed be notified within 60 days after discovery of a data breach.

- The FERPA provides students and their parents with specific rights regarding the release of student records.
- The COPPA requires websites that cater to children to offer comprehensive privacy policies, notify parents or guardians about their data collection practices, and receive parental consent before collecting any personal information from children under the age of 13.
- Title III of the Omnibus Crime Control and Safe Streets Act (also known as the Wiretap Act) regulates the interception of wire (telephone) and oral communications.
- The FISA describes procedures for the electronic surveillance and collection of foreign intelligence information between foreign powers and agents of foreign powers.
- Executive Order 12333 identifies the various government intelligence-gathering agencies and defines what information can be collected, retained, and disseminated by the agencies. It allows for the tangential collection of U.S. citizen data—even when those citizens are not specifically targeted.
- The ECPA deals with the protection of communications while in transit from sender to receiver; the protection of communications held in electronic storage; and the prohibition of devices from recording dialing, routing, addressing, and signaling information without a search warrant.
- The CALEA requires the telecommunications industry to build tools into its products that federal investigators can use—after gaining a court order—to eavesdrop on conversations and intercept electronic communications.
- The USA PATRIOT Act modified 15 existing statutes and gave sweeping new powers both to domestic law enforcement and to international intelligence agencies, including increasing the ability of law enforcement agencies to eavesdrop on telephone communication, intercept email messages, and search medical, financial, and other records; the act also eased restrictions on foreign intelligence gathering in the United States.
- The Foreign Intelligence Surveillance Act Amendments Act of 2004 authorized intelligence gathering on individuals not affiliated with any known terrorist organization (so-called lone wolves).
- The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 granted the NSA expanded authority to collect, without court-approved warrants, international communications as they flow through the U.S. telecommunications equipment and facilities.
- The PATRIOT Sunsets Extension Act granted a four-year extension of provisions of the USA PATRIOT Act that allowed roving wiretaps and searches of business records. It also extended authorization intelligence gathering on “lone wolves.”
- USA Freedom Act terminated the bulk collection of telephone metadata by the NSA instead requiring telecommunications carriers to hold the data and respond to NSA queries for data. The act also restored authorization for roving wiretaps and the tracking of lone wolf terrorists.
- “Fair information practices” is a term for a set of guidelines that govern the collection and use of personal data. Various organizations as well as countries have developed their own set of such guidelines and call them by different names.
- The OECD for the Protection of Privacy and Transborder Data Flows of Personal Data created a set of fair information practices that are often held up as the model for organizations to adopt for the ethical treatment of consumer data.
- The European Union Data Protection Directive requires member countries to ensure that data transferred to non-EU countries is protected. It also bars the export of data to countries that do not have data privacy protection standards comparable to those of the EU.

After the passage of this directive, the EU and the United States worked out an agreement that allowed U.S. companies that were certified as meeting certain "safe harbor" principles to process and store data of European consumers and companies.

- The European–United States Privacy Shield Data Transfer Program Guidelines is a stopgap measure that allows businesses to transfer personal data about European citizens to the United States. The guidelines were established after the European Court of Justice declared invalid the Safe Harbor agreement between the EU and the United States.
- The GDPR takes effect in May 2018 and addresses the export of personal data outside the EU enabling citizens to see and correct their personal data, standardizing data privacy regulations within the EU, and establishing substantial penalties for violation of its guidelines.
- The FOIA grants citizens the right to access certain information and records of the federal government upon request.
- The Privacy Act prohibits U.S. government agencies from concealing the existence of any personal data record-keeping system.

What are the various strategies for consumer profiling, and what are the associated ethical issues?

- Companies use many different methods to collect personal data about visitors to their websites, including depositing cookies on visitors' hard drives.
- Consumer data privacy has become a major marketing issue—companies that cannot protect or do not respect customer information have lost business and have become defendants in class actions stemming from privacy violations.
- A data breach is the unintended release of sensitive data or the access of sensitive data (e.g., credit card numbers, health insurance member ids, and Social Security numbers) by unauthorized individuals. The increasing number of data breaches is alarming, as is the lack of initiative by some companies in informing the people whose data are stolen. A number of states have passed data breach notifications laws that require companies to notify affected customers on a timely basis.

What is e-discovery, and how is it being used?

- Discovery is part of the pretrial phase of a lawsuit in which each party can obtain evidence from the other party by various means, including requests for the production of documents.
- E-discovery is the collection, preparation, review, and production of electronically stored information for use in criminal and civil actions and proceedings.
- Predictive coding is a process that couples human intelligence with computer-driven concept searching in order to "train" document review software to recognize relevant documents within a document universe.

Why and how are employers increasingly using workplace monitoring?

- Many organizations have developed IT usage policies to protect against employee abuses that can reduce worker productivity and expose employers to harassment lawsuits.
- About 80 percent of U.S. firms record and review employee communications and activities on the job, including phone calls, email, web surfing, and computer files.
- The use of fitness trackers in the workplace has opened up potential new legal and ethical issues.

What are the capabilities of advanced surveillance technologies, and what ethical issues do they raise?

- Surveillance cameras are used in major cities around the world to deter crime and terrorist activities. Critics believe that such security is a violation of civil liberties.
- An EDR is a device that records vehicle and occupant data for a few seconds before, during, and after any vehicle crash that is severe enough to deploy the vehicle's air bags. The fact that most cars now come equipped with an EDR and that the data from this device may be used as evidence in a court of law is not broadly known by the public.
- Stalking apps can be downloaded onto a person's cell phone, making it possible to perform location tracking, record calls and conversations, view every text and photograph sent or received, and record the URLs of any website visited on that phone.

Key Terms

American Recovery and Reinvestment Act

Bill of Rights

Children's Online Privacy Protection Act (COPPA)

Communications Assistance for Law Enforcement Act (CALEA)

cookie

cyberloafing

Electronic Communications Privacy Act (ECPA)

electronic discovery (e-discovery)

electronically stored information (ESI)

European Union Data Protection Directive

Fair and Accurate Credit Transactions Act

Fair Credit Reporting Act

fair information practices

Family Educational Rights and Privacy Act (FERPA)

FISA Court

foreign intelligence

Foreign Intelligence Surveillance Act (FISA)

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008

Fourth Amendment

Freedom of Information Act (FOIA)

Gramm-Leach-Bliley Act (GLBA)

Health Insurance Portability and Accountability Act (HIPAA)

information privacy

litigation hold notice

National Security Letter (NSL)

NSL gag provision

opt in

opt out

PATRIOT Sunsets Extension Act of 2011

pen register

predictive coding

Privacy Act

right of privacy

Right to Financial Privacy Act

stalking app

Title III of the Omnibus Crime Control and Safe Streets Act

transborder data flow

trap and trace

U.S. person

USA Freedom Act

USA PATRIOT Act

vehicle event data recorder (EDR)

Wiretap Act

Self-Assessment Questions

What is the right of privacy, and what is the basis for protecting personal privacy under the law?

1. The Supreme Court has stated that American citizens are protected by the Fourth Amendment with no exception. True or False?

2. ______________ is a system employed to collect Internet data including search histories, photos sent and received; the contents of email, file transfers, and voice and video chats; and other Internet communication data.

   a. MYSTIC

   b. Stingray

   c. PRISM

   d. ALPR

3. Although a number of independent laws and acts have been implemented over time, no single, overarching data privacy policy has been developed in the United States. However, there is an established advisory agency that recommends acceptable privacy practices to U.S. businesses. True or False?

What are some of the laws that provide protection for the privacy of personal data, and what are some of the associated ethical issues?

4. This act allows consumers to request and obtain a free credit report once each year from each of the three primary consumer credit reporting companies.

   a. Fair Credit Reporting Act

   b. Right to Financial Privacy Act

   c. Gramm-Leach-Bliley Act

   d. Fair and Accurate Credit Transactions Act

5. Under (the) ______________, the presumption is that a student's records are private and not available to the public without the consent of the student.

   a. HIPAA

   b. American Recovery and Reinvestment Act

   c. Family Educational Rights and Privacy Act

   d. Children's Online Privacy Protection Act

6. ______________ describes procedures for the electronic surveillance and collection of foreign intelligence between foreign powers and agents of foreign powers. It also created a special court which meets in secret to hear applications for orders approving electronic surveillance anywhere within the United States.

   a. The Foreign Intelligence Surveillance Act

   b. The USA PATRIOT Act

   c. The USA Freedom Act

   d. Executive Order 12333

7. (The) ______________ approves the use of any intelligence collection techniques that are in accordance with procedures established by the head of the intelligence community and approved by the attorney general.
   a. Foreign Intelligence Surveillance Act
   b. USA PATRIOT Act
   c. USA Freedom Act
   d. Executive Order 12333
8. The number of U.S. government intelligence-gathering units identified in Executive Order 12333 exceeds 18. True or False?
9. The ______________ is designed to strengthen the data protection for individuals within the EU and includes stiff penalties for privacy violations.
   a. Organization for Economic Co-operation and Development for the Protection of Privacy and Transborder Flows of Personal Data
   b. European Union Data Protective Directive
   c. European–United States Privacy Shield Data Transfer Program Guidelines
   d. General Data Protection Regulation
10. Federal agencies receiving a ______________ request must acknowledge that the request has been received and indicate when the request will be fulfilled, with an initial response within 20 working days unless an unusual circumstance occurs.

What are the various strategies for consumer profiling, and what are the associated ethical issues?

11. Many companies obtain information about web surfers through the use of ______________, which are text files that can be downloaded to the hard drives of users so that the website is able to identify visitors on subsequent visits.
12. Publicly traded organizations have an obligation to report all data breaches to the Securities and Exchange Commission. True or False?

What is e-discovery, and how is it being used?

13. Often organizations who are engaged in litigation will send a ______________ notice to its employees or to the opposing party to save relevant data and to suspend data that might be due to be destroyed based on normal data-retention rules.
14. ______________ is a process that couples human guidance with computer-driven concept searching in order to train document review software to recognize relevant documents with a document universe.

Why and how are employers increasingly using workplace monitoring?

15. A recent study revealed that between ______________ percent of workers' time online has nothing to do with work.
    a. 20 and 40
    b. 30 and 50
    c. 50 and 70
    d. 60 and 80

16. The Fourth Amendment cannot be used to limit how a private employer treats its employees, and private-sector employees must seek legal protection against an invasive employer under various state statues. True or False?

What are the capabilities of advanced surveillance technologies, and what ethical issues do they raise?

17. China has more surveillance cameras per person than Great Britain. True or False?
18. Beginning with the model year 2011 vehicles, the National Highway Safety Administration defined a minimum set of 15 data elements that must be captured for manufacturers who voluntarily install Electronic Data Recorders on their vehicles. True or False?

Self-Assessment Answers

1. False; 2. c; 3. False; 4. d; 5. c; 6. a; 7. d; 8. True; 9. d; 10. Freedom of Information Request; 11. cookies; 12. False; 13. litigation hold; 14. Predictive coding; 15. d; 16. True; 17. False; 18. True

Discussion Questions

1. For some people, knowing that 21 different government agencies are authorized to gather intelligence data provides them with a sense of security. Others believe that this creates a significant opportunity for duplication of effort and wasted resources. Still others are concerned that everything about them and what they do is known by the government. Choose one side of this issue and defend your position.
2. Prepare a set of arguments that would support the contention that the USA PATRIOT Act was overreaching in both its scope and its approach. Then prepare a set of arguments that support the USA PATRIOT Act as an effective and appropriate way to protect the United States from further terrorist acts.
3. Do you think a FOIA request from an average citizen for information about the process by which potential drone targets are selected and approved should be granted? Why or why not?
4. Go to the website of one of the three primary consumer credit reporting companies (Equifax, Experian, or TransUnion). Find the instructions to request a free credit report, and do so. How long did it take to receive your free credit report? Is there information on the report you to believe to be in error? Check the website and credit report to find out how can you dispute any information which you believe is an error.
5. Do research to gather and summarize the key facts in *Katz v. United States*. Do you agree with the Supreme Court's ruling in this case? Why did this case set such an important precedent?
6. What is predictive coding? How is it different from doing key word searches on documents? What are the key issues to weigh when considering use of predictive coding?
7. Do you believe it is acceptable for a website to assume that consumers are okay with any changes the site makes to it privacy policy unless they explicitly take action to opt out? Explain your reasoning.
8. Should some sort of congressional approval or review process be established for executive orders? Why or why not?

9. What is the difference between a pen register and a trap and trace? What is required in order for a law enforcement agency to gain approval for use of one of these measures?
10. What are the main reasons employers monitor workers? Provide examples of three types of employee monitoring that you feel are justified. Provide three examples of three types of employee monitoring you feel are not justified.
11. Do you think that law enforcement agencies should be able to use advanced surveillance cameras and data from vehicle data recorders in a court of law? Why or why not?
12. Do you think that the installation of stalker software on suspects' cell phones should be authorized for law enforcement agencies? If so, under what circumstances should such use be permitted? If not, why not.

What Would You Do?

Use the five-step decision-making process discussed in Chapter 1 to analyze the following situations and recommend a course of action.

1. You are the webmaster for a site that caters to young children. What measures must you take to ensure that your website does not violate the Children's Online Privacy Protection Act?
2. Your friend is going through a tough time with his current significant other and believes she is cheating on him. He is aware of your technical prowess and has asked you to help him purchase and install a stalking app on her cell phone. What would you say?
3. You are a recent college graduate with only a year of experience with your employer. You were recently promoted to manager of email services. You are quite surprised to receive a phone call at home on a Saturday from the Chief Financial Officer of the firm asking that you immediately delete all email from all email servers, including the archive and back-up servers, that is older than six months. She states that the reason for her request is that there have been an increasing number of complaints about the slowness of email services. In addition, she says she is concerned about the cost of storing so much email. This does not sound right to you because you recently have taken several measures that have speeded up email services. An alarm goes off when you recall muted conversations in the lunchroom last week about an officer of the company passing along insider trader information to an executive at a hedge fund. What do you say to the Chief Financial Officer?
4. Your auto insurance company has offered you a 15 percent discount (roughly $200 per year) if you agree to let them install a sophisticated vehicle event data recorder (EDR) in your car. You have read over the terms of the agreement and discover that if you are involved in an accident, you must agree to let the data from the device be collected and analyzed by a third-party accident investigation firm. You must also agree to let findings from this analysis be used in a court of law. What questions would you want answered and what advice might you seek before deciding whether to accept this discount offer?
5. You are the general manager of a luxury car dealership. You are considering purchasing data from a data broker that collects data of high potential value to your dealership. In addition to providing a list of names, mailing addresses, and email addresses, the data include an approximate estimate of individuals' annual income based on the zip code in

which they live, census data, and highest level of education achieved. Using the data provided by the broker, you could establish an estimated annual income for each person on the list to identify likely purchasers of your dealership's autos and then send emails to those potential customers. List the advantages and disadvantages of such a marketing strategy. Would you recommend this means of promotion in this instance? Why or why not?

Cases

1. Serious Data Breach at OPM

The U.S. Office of Personnel Management (OPM) is an independent agency of the U.S. government that assists other federal agencies in hiring new employees, conducting background check investigations, and managing pension benefits for retired federal employees and their families. The agency maintains data on millions of federal government employees, retirees, contractors, and prospective employees. These data were recently compromised in two separate but related data breaches at the OPM, raising concerns not only about potential identity theft and blackmail but also about the possible use of that data in intelligence operations launched against the United States.

Early in 2015, OPM discovered that the personnel data (full name, birth date, home address, and Social Security numbers) of 4.2 million current and former federal government employees had been stolen. Then, in June 2015, OPM announced that the background investigation records of 21.5 million current, former, and prospective federal employees and contractors had been stolen as the result of a second data breach.

During a hearing in front of the House Oversight and Reform Committee shortly after the second breach was announced, OPM's Chief Information Officer Donna Seymour acknowledged that the information compromised in the data breach included “SF-86 data as well as clearance adjudication information.” Current and prospective federal employees and service members who require a security clearance must complete the SF-86, a 127-page questionnaire, which asks for information about family members, friends, employment history, foreign travel, interactions with foreign nationals, details on alcohol and drug use, mental illness, credit ratings, bankruptcies, arrest records, and court actions. The document also includes information from record checks with local law enforcement where the individual lived, worked, or went to school during the previous 10 years.

Adjudication information includes additional personal information that is gathered for all “persons being considered for initial or continued eligibility for access to classified information.” The information is obtained through personal interviews not only with the applicant but also with educators, employers, neighbors, references, roommates, significant others, and spouses of the applicant. Adjudication information can include revelations about past sexual behavior, personal debt, specific reasons for a divorce, and information about a history of addictions, among other details. The adjudication data that were breached at the OPM also included actual fingerprint data for more than 5.6 million people.

While the personally identifiable information exposed in the intrusion creates a risk of identity theft, security experts are more concerned that a nation or even a criminal organization could use the information to run intelligence operations against the United States on a massive and unprecedented scale. Some of the issues of particular concern to security experts include the following:

- Because the Central Intelligence Agency (CIA) conducts its own background checks on potential employees, and did not manage the process through the OPM, any State Department employees whose data were not stolen in the OPM data breach could be identified as likely agents of the CIA.
- The perpetrators of the data breach could have tampered with the data and granted security clearances to people who not only didn't actually warrant them, but who might have been recruited in advance to work for the attackers.
- The sensitive personnel information data gathered could be used to "neutralize" U.S. agents and officials by exploiting their personal weaknesses and/or targeting their relatives abroad.

After the breaches were announced, the U.S. Department of Defense and OPM awarded a $133 million contract to Identity Theft Guard Solutions LLC to provide 10 years of credit monitoring and identity theft protection for the 21.5 million individuals whose personal information was stolen. However, when information about spouses, children, significant others, and people who are listed as references on the security clearance records is factored in, the number of people whose personally identifiable information was compromised is likely in the range of 78 million to 276 million people. Not all these additional people were offered identity theft protection.

In June 2015, the American Federation of Government Employees (AFGE), the country's largest government employee union, filed a class action lawsuit in U.S. district court against the agency, OPM Director Katherine Archuleta, OPM Chief Information Officer Donna Seymour, and KeyPoint Government Solutions, the contractor hired by OPM to conduct the background investigations. The American Federation of Government Employees says OPM and the contractor violated the Privacy Act by neglecting to secure employees' personal data (even after repeated warnings about its data security practices), which resulted in financial and emotional harm for those employees.

While claims alleging OPM's failure to protect workers' data could hold up in court, proving damages have actually been suffered will likely be more difficult. The precedent used by courts deciding on issues related to "fear of prospective losses" (which is the basis of the AFGE lawsuit) has been a 2013 decision, *Clapper v. Amnesty International USA*. In that case, journalists and human rights advocates unsuccessfully sued for damages related to the cost and inconvenience of protecting themselves against the possibility of warrantless digital surveillance authorized by the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008. They claimed that they engage in sensitive international communications with individuals who they believe are likely targets of surveillance authorized under §1881a of the Amendments Act. The Supreme Court ruled that they could not show that they suffered injury that was "particularized, and actual or imminent, fairly traceable to the challenged action, and addressable by a favorable ruling."[83] As a result, the plaintiffs lacked standing and the lawsuit was thrown out of court.

The claims of the plaintiff in the AFGE lawsuit are likely to be bolstered in part by finding in a report from the U.S. House of Representatives' Committee on Oversight and Government Reform, which indicates that OPM did not follow rudimentary cybersecurity recommendations that could have mitigated or even prevented the attacks. According to the report, the OPM data breaches were made worse by the agency's careless security culture and ineffective leadership, which failed to employ readily available tools that could have stopped or mitigated the intrusions. The report also pointed out that the OPM had failed to act on repeated inspector general reports as far back as 2005 that warned of cybersecurity shortcomings.

OPM director Katherine Archuleta resigned a month after the breaches were announced in response to pressure from House Oversight and Government Reform Committee Chairman Jason Chaffetz. In February 2016, Donna Seymour, CIO for the Office of Personnel Management, announced her retirement. Pressure had been mounting on Seymour for her to step down, and her resignation came just two days before she was scheduled to testify again before the House committee.

OPM has claimed that it achieved "significant progress" in improving cybersecurity on its systems following the data breaches. The agency has implemented multifactor authentication, modernized its information technology infrastructure, appointed a new senior cybersecurity adviser, and formed a new organization responsible for background checks on employees and contractors. That new entity, the National Background Investigations Bureau (NBIB), which became operational in October 2016, runs on information systems that are managed by the Pentagon.

Critical Thinking Questions

1. Do you feel there should be some sort of redress for the 21 million people whose personal information was stolen even if they cannot prove actual monetary damages?
2. How might foreign powers and/or terrorists use the stolen data to mount intelligence operations against the United States?
3. Go online to do research on the steps OPM has taken to improve its cybersecurity? Are you satisfied with these actions? If not, what additional changes would you suggest?

Sources: "Cybersecurity Resource Center: What Happened," OPM.gov, https://www.opm.gov/cybersecurity/cybersecurity-incidents/ (accessed December 5, 2016); David Larter and Andrew Tilghman, "Military Clearance OPM Data Breach 'Absolute Calamity'," *Navy Times*, June 17, 2015, https://www.navytimes.com/story/military/2015/06/17/sf-86-security-clearance-breach-troops-affected-opm/28866125/; Aliya Sternstein, "Why the Lawsuit Against OPM over the Massive Data Breach Faces an Uphill Battle," Next Gov, July 1, 2015, www.nextgov.com/security/2015/07/why-lawsuit-against-opm-over-massive-data-breach-faces-uphill-battle/116701/; Michael Adams, "Why the OPM Hack Is Far Worse Than You Imagine," LawFare, March 11, 2016, https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine; Andrea Peterson, "OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought," *Washington Post*, September 23, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?utm_term=.5fc234f4937a; "Cybersecurity Resource Center: Sign Up for Services," OPM.gov, https://www.opm.gov/cybersecurity/ (accessed December 6, 2016); Ian Smith, "OPM CIO Donna Seymour Resigns," FedSmith, February 22, 2016, www.fedsmith.com/2016/02/22/opm-cio-donna-seymour-resigns/.

2. Time to Update the Electronic Communications Privacy Act?

As discussed in the chapter, the Electronic Communications Privacy Act (ECPA) deals with three main issues: (1) the protection of communications while in transfer from sender to receiver; (2) the protection of communications held in electronic storage; and (3) the prohibition of devices from recording dialing, routing, addressing, and signaling information without a search warrant. The ECPA makes it a crime to intercept or obtain electronic communications unless otherwise provided for under law or an exception to ECPA.

While the ECPA provides many important and useful protections, much of today's communications technology was not even available when the act was enacted more than 30 years ago—ubiquitous personal computers, the Internet and the World Wide Web, mobile computing and communications devices, social networks, and cloud computing. Nor was email used as widely as it is now so emails were sent and received with little thought about the need to preserve them nor did people ever consider that emails might be saved on servers somewhere and be subject to a search warrant.

Under 18 U.S.C. § 2703(d) of the ECPA, law enforcement can obtain a court order—called a 2703(d) order—to compel a computer service provider (e.g., a cloud computing service provider, social network operator, or email service provider) to disclose detailed records about a customer's or subscriber's use of services, such as account activity logs that reflect what Internet protocol (IP) addresses the subscriber visited over time, the addresses of others from and to whom the subscriber exchanged email, and contact lists. The ECPA also provides for gag orders, which direct the recipient of a 2703(d) order to refrain from disclosing the existence of the order or the investigation. This means that a computer service provider served with such an order cannot inform its customers that their emails are being searched. The government has issued hundreds of thousands of such NSLs accompanied with gag orders.

As part of a drug investigation, in December 2013, the federal government applied for a search warrant under a 2703(d) order to obtain the contents of emails and other details from a user account hosted by Microsoft. While the noncontent data were stored in the United States, the contents of the emails were stored on one of Microsoft's servers located in Dublin, Ireland. Microsoft refused to turn the emails over to the government, arguing that email stored on computer servers in another country cannot be obtained through a warrant issued by a U.S. court because the reach of such a warrant does not extend beyond the United States. This position was supported by several other technology companies, including rivals of Microsoft. After a two-year battle, a U.S. appeals court panel ruled in Microsoft's favor. If this ruling had gone against Microsoft, U.S. law enforcement would have been given jurisdiction to access digital content stored by U.S. companies, no matter where in the world it was stored. Such approval could have jeopardized the future of international cloud computing as well as other computer services.

In a separate, but related case, in April 2016, Microsoft sued the U.S. government for the right to inform its customers when a federal agency is examining its customers' emails. Over a period of 18 months ending in March 2016, Microsoft received more than 5,600 2703(d) orders, nearly half of which barred Microsoft from informing its customers that the government was seeking their data through warrants, subpoenas, and other requests. Microsoft asserted that these gag orders violated its First Amendment right to inform its customers about the search of their files. In addition, Microsoft charged that law enforcement use of gag orders "flouts" Fourth Amendment requirements that the government provide notice to people when their property is being searched or seized. In the suit, Microsuit argued that "people do not give up their rights when they move their private information to the cloud," Microsoft further argued that the federal government "has exploited the transition to cloud computing as a means of expanding its power to conduct secret investigations." Over two dozen technology and media organizations filed briefs in support of Microsoft in this case, including Apple, Amazon, Fox News, Google, National Public Radio, the *Washington Post*, and Yahoo.

Critical Thinking Questions

1. Do you believe that it is time to consider changes to the ECPA to bring it more in line with the Bill of Rights, or do you believe that concerns about terrorism and crime justify efforts to revise the Bill of Rights?
2. Congress proposed legislation in both 2013 and 2015 to revise the ECPA; however, the changes never made it through the legislative process. Do research and write a brief summary explaining why no action was taken.
3. Why do you think media organizations would support Microsoft in its suits against the United States over the provisions of the ECPA?

Sources: Sarah McBride, "Microsoft Sues U.S. Government Over Data Requests," Reuters, April 15, 2016, www.reuters.com/article/us-microsoft-privacy-idUSKCN0XB22U; Jay Greene, "Companies Back Microsoft's Effort to Alert Users When Authorities Seek Their Data," *Wall Street Journal*, September 2, 2016, www.wsj.com/articles/companies-back-microsofts-effort-to-alert-users-when-authorities-seek-their-data-1472865604; "Tech Companies Back Microsoft in Ireland Email Warrant Case," *NBC News*, December 15, 2014, www.nbcnews.com/tech/tech-news/tech-companies-back-microsoft-ireland-email-warrant-case-n268901; Hanni Fakhoury, "The Faulty Logic at the Heart of Microsoft Ireland Email Dispute," Electronic Frontier Foundation, December 15, 2014, https://www.eff.org/deeplinks/2014/12/faulty-logic-heart-microsoft-ireland-email-dispute.

End Notes

[1] David McLaughlin and Stephanie Bodoni, "Facebook's WhatsApp Privacy Changes Raise EU, U.S. Concerns," Bloomberg, August 29, 2016, https://www.bloomberg.com/news/articles/2016-08-29/whatsapp-privacy-changes-raise-eu-concern-over-user-data-control.

[2] Natasha Lomas, "WhatsApp's Privacy U-turn on Sharing Data with Facebook Draws More Heat in Europe," *TechCrunch*, September 30, 2016, https://techcrunch.com/2016/09/30/whatsapps-privacy-u-turn-on-sharing-data-with-facebook-draws-more-heat-in-europe.

[3] "Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission," Privacy Protection Study Commission, July 12, 1977, http://aspe.hhs.gov/datacncl/1977privacy/toc.htm.

[4] "NSA Reportedly Recording All Phone Calls in a Foreign Country," *Associated Press*, March 19, 2014, www.foxnews.com/politics/2014/03/19/nsa-reportedly-recording-all-phone-calls-in-foreign-country/.

[5] Kia Makarechi, "Julian Assange Goes Where Glenn Greenwald Wouldn't," *Vanity Fair*, May 19, 2014, www.vanityfair.com/online/daily/2014/05/julian-assange-glenn-greenwald-nsa-afghanistan.

[6] *Olmstead v. United States*, 277 U.S. 438 (1928), www.law.cornell.edu/supct/html/historics/USSC_CR_0277_0438_ZS.html (accessed December 19, 2012).

[7] Roger Clarke, "Introduction to Dataveillance and Information Privacy and Definition of Terms," August 15, 1997, www.rogerclarke.com/DV/Intro.html#Priv (accessed December 19, 2012).

[8] "The Fair Credit Reporting Act," www.ftc.gov/os/statutes/031224fcra.pdf (accessed December 19, 2016).

[9] U.S. Government Publishing Office, "Gramm-Leach-Bliley Act," www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf (accessed November 29, 2016).

[10] "FAST Act Amends Gramm-Leach-Bliley Act," Frontline Compliance, December 15, 2015, http://frontlinecompliance.com/fast-act-amends-gramm-leach-bliley-act/.

[11] U.S. Government Publishing Office, "Fair and Accurate Credit Transactions Act," www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf (accessed November 29, 2016).

[12] George V. Hulme, "Protecting Privacy," *InformationWeek*, April 16, 2001.

[13] "Data Breach Results in $4.8 Million HIPAA Settlements," U.S. Department of Health and Human Services, May 7, 2014, www.hhs.gov/about/news/2014/05/07/data-breach-results-48-million-hipaa-settlements.html.

[14] "Office of Civil Rights," U.S. Department of Health and Human Services, www.hhs.gov/ocr/office/about-us/index.html (accessed November 27, 2016).

[15] "HIPAA Creating Barriers to Research and Discovery," Association of Academic Health Centers, http://www.aahcdc.org/policy/reddot/AAHC_HIPAA_Creating_Barriers.pdf (accessed December 26, 2016).

[16] Kelly Wallace, "How Much Time Do Parents Spend on Screens? As Much as Their Teens," CNN, December 6, 2016, http://www.cnn.com/2016/12/06/health/parents-screen-use-attitudes-tweens-teens/index.html.

[17] Thaddeus Ferber and Danielle Evennou, "First Look: New FERPA Regulations," The Forum for Youth Investment, December 2, 2011, http://forumfyi.org/files/First_Look_FERPA.pdf.

[18] Joseph Remines, "Four Major Toy Companies Fined for Violating the COPPA," The Merkle, September 16, 2016, http://themerkle.com/four-major-toy-companies-fined-for-violating-the-coppa/.

[19] "A.G. Schneiderman Announces Results of 'Operation Child Tracker,' Ending Illegal Online Tracking of Children at Some of Nation's Most Popular Kids' Websites," New York State Office of the Attorney General, September 13, 2016, www.ag.ny.gov/press-release/ag-schneiderman-announces-results-operation-child-tracker-ending-illegal-online.

[20] "Privacy & Civil Liberties: Title III of the Omnibus of the Crime and Safe Streets Act of 1968 (Wiretap Act)," U.S. Department of Justice, www.it.ojp.gov/default.aspx?area=privacy&page=1284 (accessed November 29, 2016).

[21] *Katz v. United States*, 389 U.S. 247 (1967), http://supreme.justia.com/cases/federal/us/389/347/case.html (accessed November 27, 2016).

[22] "Wire Tap Report," United States Courts, December 31, 2015, www.uscourts.gov/statistics-reports/wiretap-report-2015.

[23] "Federal Statutes Important in the Information Sharing Environment (ISE)," U.S. Department of Justice, www.it.ojp.gov/default.aspx?area=privacy&page=1286 (accessed November 26, 2016).

[24] "Foreign Intelligence Surveillance Act Court Orders 1979–2015," Electronic Privacy Information Center, https://epic.org/privacy/surveillance/fisa/stats/default.html (accessed November 23, 2016).

[25] Zach Walton, “Law Enforcement Now Wants Wireless Carriers to Store Your Text Messages as Evidence,” *Web Pro News*, December 3, 2012, www.webpronews.com/law-enforcement-now-wants-wireless-carriers-to-store-your-text-messages-for-evidence-2012-12.

[26] “Communications Assistance for Law Enforcement Act (CALEA),” Federal Communications Commission, http://transition.fcc.gov/calea (accessed November 28, 2016).

[27] “*Doe v. Holder*,” American Civil Liberties Union, November 17, 2009, www.aclu.org/cases/doe-v-holder.

[28] Mike Masnick, “Court Says National Security Letters Are Now Constitutional Under USA Freedom Act,” Tech Dirt, April 22, 2016, https://www.techdirt.com/articles/20160421/16473934241/court-says-national-security-letters-are-now-constitutional-under-usa-freedom-act.shtml.

[29] James Risen and Eric Lichtblau, “Bush Lets U.S. Spy on Callers Without Courts,” *New York Times*, December 16, 2005, www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

[30] Eric Lichtblau and James Risen, “Officials Say U.S. Wiretaps Exceeded Law,” *New York Times*, April 16, 2009, www.nytimes.com/2009/04/16/us/16nsa.html.

[31] Eric Lichtblau and James Risen, “Officials Say U.S. Wiretaps Exceeded Law,” *New York Times*, April 16, 2009, www.nytimes.com/2009/04/16/us/16nsa.html.

[32] “Edward Snowden: Leaks that Exposed US Spy Programme,” BBC News, January 14, 2014, http://www.bbc.com/news/world-us-canada-23123964.

[33] Editorial Board, “Edward Snowden, Whistle-Blower,” *New York Times*, January 1, 2014, https://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html?_r=0.

[34] “About the OECD,” The Organisation for Economic Co-Operation and Development, www.oecd.org/about (accessed November 29, 2016).

[35] “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” The Organisation for Economic Co-Operation and Development, www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (accessed November 28, 2016).

[36] “European Commission Finds New Zealand’s Data Protection Law Provides Adequate Safeguards,” Hunton & Williams LLP, December 20, 2012, www.huntonprivacyblog.com/tag/eu-data-protection-directive.

[37] Rebecca Herold, “European Union (EU) Data Protection Directive of 1995: Frequently Asked Questions,” InformationShield, May 2002, www.informationshield.com/papers/EU%20Data%20Protection%20Directive%20FAQ.pdf.

[38] “Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks,” Export.gov, www.export.gov/safeharbor (accessed November 26, 2016).

[39] Ellen Nakashima, “Top E.U. Court Strikes Down Major Data-Sharing Pact Between U.S. and Europe,” *Washington Post*, December 6, 2015, https://www.washingtonpost.com/world/national-security/eu-court-strikes-down-safe-harbor-data-transfer-deal-over-privacy-concerns/2015/10/06/2da2d9f6-6c2a-11e5-b31c-d80d62b53e28_story.html?utm_term=.b7d5b11358ac.

[40] "EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield, European Commission," February 2, 2016, http://europa.eu/rapid/press-release_IP-16-216_en.htm.

[41] David Moncure, John Del Piero, and Jeffrey McKenna, "The General Data Protection Regulation's Key Implications for E-Discovery," *Inside Counsel*, November 23, 2016, www.insidecounsel.com/2016/11/23/the-general-data-protection-regulations-key-implic.

[42] Dana Heide, "U.S. Companies Slow to Adopt European Data Transfer Agreement," *Wall Street Journal*, August 14, 2016, www.wsj.com/articles/u-s-companies-slow-to-adopt-european-data-transfer-agreement-1471196672.

[43] Ben Martin and James Titcomb, "Regulators Could Fine Tesco Bank Over Cyber Attack" *Telegraph*, November 7, 2016, www.telegraph.co.uk/business/2016/11/07/tesco-bank-to-freeze-customer-transactions-after-hacking-attack/.

[44] "Tesco Could Be Facing £2bn Fine for Breach Under GDPR," dataIQ, November 9, 2016, www.dataiq.co.uk/news/tesco-could-be-facing-ps2bn-fine-breach-under-gdpr.

[45] "FOIA," www.fcc.gov/foia, Federal Communications Commission (accessed November 30, 2016).

[46] "What Is FOIA?" FOIA.gov, https://www.FOIA.gov (accessed November 29, 2016).

[47] "What Are FOIA Exemptions?" FOIA.gov, https://www.foia.gov/faq.html#exemptions (accessed November 29, 2016).

[48] Luke O'Neil, "Why Is the DEA Not Cooperating with This FOIA Request?" *Esquire*, December 2, 2015, www.esquire.com/news-politics/a40126/phil-eil-dea-lawsuit/.

[49] Mark Schieldrop, "RI Journalist Wins Landmark FOIA Case Against DEA, Justice Department," *Cranston Patch*, September 16, 2016, http://patch.com/rhode-island/cranston/ri-journalist-wins-landmark-foia-case-against-dea-justice-department.

[50] Sarah Westwood, "Amazing Ways Feds Hide Info," *Washington Examiner*, March 16, 2015, www.washingtonexaminer.com/amazing-ways-feds-hide-info/article/2561655.

[51] Luke O'Neil, "Why Is the DEA Not Cooperating with This FOIA Request?" *Esquire*, December 2, 2015, www.esquire.com/news-politics/a40126/phil-eil-dea-lawsuit/.

[52] "The Privacy Act of 1974," Electronic Privacy Information Center, http://epic.org/privacy/1974act (accessed November 30, 2016).

[53] Marianne Kolbasuk McGee, "Most Claims in TRICARE Breach Dismissed," *Data Breach Today*, May 12, 2014, www.databreachtoday.com/most-claims-in-tricare-breach-dismissed-a-6834.

[54] Aliya Sternstein, "Why the Lawsuit Against OPM Over the Massive Data Breach Faces an Uphill Battle," *Next Gov*, July 1, 2015, www.nextgov.com/security/2015/07/why-lawsuit-against-opm-over-massive-data-breach-faces-uphill-battle/116701/.

[55] Elizabeth Palermo and Paul Wagenseil, "10 Worst Data Breaches of All Time," *Tom's Guide*, December 16, 2016, www.tomsguide.com/us/biggest-data-breaches,news-19083.html.

[56] Robert McMillan, "Yahoo Says Information on at Least 500 Million User Accounts Was Stolen," *Wall Street Journal*, September 22, 2016, www.wsj.com/articles/yahoo-says-information-on-at-least-500-million-user-accounts-is-stolen-1474569637?mod=trending_now_2.

[57] "Target Data Breach Cost for Banks Tops $200M," *NBC News*, February 18, 2014, www.nbcnews.com/business/business-news/target-data-breach-cost-banks-tops-200m-n33156.

[58] Noor Us Subah, "How Target Corporation (TGT) Recovered From Last Year‘s Credit-Card Breach," BidnessEtc, November 20, 2014, www.bidnessetc.com/29547-how-target-corporation-tgt-recovered-from-last-years-creditcard-breach/.

[59] Elizabeth A. Harris, "Data Breach Hurts Profit at Target," *New York Times*, February 26, 2014, www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html.

[60] "Target Data Breach Cost for Banks Tops $200M," *NBC News*, February 18, 2014, www.nbcnews.com/business/business-news/target-data-breach-cost-banks-tops-200m-n33156.

[61] Tim Greene, "Anthem Hack: Personal Data Stolen Sells for 10× Price of Stolen Credit Card Numbers," *Network World*, February 6, 2015, www.networkworld.com/article/2880366/security0/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[62] Tatyana Shumsky, "Corporate Judgment Call: When to Disclose You've Been Hacked," *Wall Street Journal*, September 19, 2016, www.wsj.com/articles/corporate-judgment-call-when-to-disclose-youve-been-hacked-1474320689.

[63] Tatyana Shumsky, "Corporate Judgment Call: When to Disclose You've Been Hacked," *Wall Street Journal*, September 19, 2016, www.wsj.com/articles/corporate-judgment-call-when-to-disclose-youve-been-hacked-1474320689.

[64] John Rebeiro, "Trump Hotels Fined over Data Breaches," Computerworld, September 27, 2016, www.computerworld.com/article/3123001/security/trump-hotel-chain-fined-over-data-breaches.html.

[65] Philip Favro, "Conducting e-Discovery in Glass Houses: Are You Prepared for the Next Stone?" *e-Discovery 2.0*, August 27, 2012, www.clearwellsystems.com/e-discovery-blog/2012/08/27/conducting-ediscovery-in-glass-houses-are-you-prepared-for-the-next-stone.

[66] "Roundtable Discussion: Changing Ethical Expectations—Navigating the Changing Ethical and Practical Expectations for E-Discovery," Presented at the Northern Kentucky University Chase College of Law Northern Kentucky Law Spring Symposium, February 28, 2009.

[67] Ben Kerschberg, "E-Discovery and the Rise of Predictive Coding," *Forbes*, March 23, 2011, www.forbes.com/sites/benkerschberg/2011/03/23/e-discovery-and-the-rise-of-predictive-coding/.

[68] Justine Hofherr, "You're 'Cyberloafing' Right Now. Here's How Your Employer Might Stop That One Day," Boston.com, March 17, 2016, http://www.boston.com/jobs/jobs-news/2016/03/17/youre-cyberloafing-right-now-heres-employer-might-stop-one-day.

[69] Katie Johnston, "Firms Step Up Employee Monitoring at Work," *Boston Globe*, February 19, 2016, https://www.bostonglobe.com/business/2016/02/18/firms-step-monitoring-employee-activities-work/2l5hoCjsEZWA0bp10BzPrN/story.html.

[70] James Temperton, “One Nation Under CCTV: The Future of Automated Surveillance,” *Wired-UK*, August 17, 2015, www.wired.co.uk/article/one-nation-under-cctv.

[71] James T. Areddy, “One Legacy of Tiananmen: China’s 100 Million Surveillance Cameras,” *Wall Street Journal*, June 5, 2014, http://blogs.wsj.com/chinarealtime/2014/06/05/one-legacy-of-tiananmen-chinas-100-million-surveillance-cameras/.

[72] Petr Knava, “Beijing Now Most-Watched City in the World; London and Chicago Look On in Envy,” Pajiba, October 5, 2015, www.pajiba.com/miscellaneous/which-cities-have-the-widest-cctv-coverage-in-the-world-.php.

[73] Lauren Petty and Charlie Wojciechowski, “Emanuel Credits Increase in Cameras for Crime on CTA Dropping by 25 Percent” *Chicago 5*, January 27, 2016, www.nbcchicago.com/news/local/Emanuel-Crime-on-CTA-Fell-by-25-Percent-366675941.html.

[74] “NYPD Unveils Crime- and Terror-Fighting ‘Domain Awareness System’,” *CBS Local*, August 8, 2012, http://newyork.cbslocal.com/2012/08/08/nypd-unveils-crime-and-terror-fighting-domain-awareness-system.

[75] Thomas H. Davenport, “How Big Data Is Helping the NYPD Solve Crimes Faster,” Fortune, July 17, 2016, http://fortune.com/2016/07/17/big-data-nypd-situational-awareness/.

[76] “NYPD’s ‘Domain Awareness’ Surveillance System Built by Microsoft, Unveiled by Bloomberg,” *Huffington Post*, August 9, 2012, www.huffingtonpost.com/2012/08/09/nypd-domain-awareness-surveillance-system-built-microsoft_n_1759976.html.

[77] Rebekah Morrison, “New York’s Domain Awareness System: Every Citizen Under Surveillance, Coming to a City Near You,” *North Carolina Journal of Law and Technology*, February 23, 2016, http://ncjolt.org/new-yorks-domain-awareness-system-every-citizen-under-surveillance-coming-to-a-city-near-you/.

[78] David Danaher, P.E., Jeff Ball, Ph.D., P.E., Trevor Buss, P.E. and Mark Kittle, P.E., “Eaton VORAD Collision Warning System,” Veritech Consulting Engineering, LLC, June 14, 2012, www.veritecheng.com/eaton-vorad-collision-warning-system.

[79] “EDR Legal Updates,” Collision Data Service, http://edraccess.com/CaseLaw.aspx (accessed January 5, 2013).

[80] *Howard v. Miami Twp*, Fire Div, 171 Ohio App.3d 184, 2007-Ohio-1508, www.sconet.state.oh.us/rod/docs/pdf/2/2007/2007-ohio-1508.pdf (accessed November 27, 2016).

[81] “High-Tech Devices Leave Users Vulnerable to Spies,” *Phys.Org*, January 5, 2012, http://phys.org/print244989742.html.

[82] “Are You Looking for the Best Spy Phone Software That Really Work?” www.spyphonesreview.com (accessed November 27, 2016).

[83] “*Clapper, Director of National Intelligence, et al. v. Amnesty International, USA et al*.,” https://www.supremecourt.gov/opinions/12pdf/11-1025_ihdj.pdf.

CHAPTER 5

FREEDOM OF EXPRESSION

QUOTE

If we don't believe in freedom of expression for people we despise, we don't believe in it at all.

—Noam Chomsky, American linguist, philosopher, cognitive scientist, historian, social critic, and political activist

Marcos Mesa Sam Wordley/Shutterstock.com

ORGANIZATIONS BEHAVING BADLY

Around the world, Internet censorship and surveillance is on the rise, fueling concerns regarding issues such as freedom of expression, privacy rights, free and fair elections, and corruption. For instance, political and human rights activists in Brazil, China, Ethiopia, Greece, India, Indonesia, Iran, Russia, Saudi Arabia, Turkey, Uganda, and Zimbabwe all are subject to particularly strong censorship and suppression. And in many countries, journalists, as well as their sources, are the targets of censorship and surveillance activities by those working on behalf of politicians, government entities, and criminals.

Faced with the reality of online censorship and surveillance, many activists, journalists, and whistle-blowers—among others—feel an increased need to keep their Internet activities concealed from the government, Internet service providers, and website operators. Those concerns were only heightened following the release of information regarding the U.S. government's surveillance activities that came to light with Edward Snowden's leak of National Security Agency documents in 2013.

One tool available for those looking for more online privacy and protection is Tor, which is marketed as a free software and an open network that can safeguard users from network surveillance that threatens their "personal freedom and privacy, confidential business activities and relationships, and state security." Tor works by bouncing Internet communications around a network of servers distributed around the world, thus thwarting anyone who is trying to monitor the user's Internet connection to learn what sites he or she is visiting while also preventing the sites being visited from establishing the user's physical location. Tor also allows website operators to publish websites without revealing their location.[1]

With features that enable users to access information, communicate freely, and form and discover communities of support in potentially dangerous environments, Tor is one example of how technology can be employed to serve the causes of freedom, safety, liberty, and human rights for people around the world. However, a recent study found that 57 percent of the sites designed for Tor are used by people engaged in criminal activity, including drugs, illicit finance, and extreme pornography.[2] What measures are available to defeat Internet censorship and surveillance so that Internet users can truly enjoy freedom of expression? Can technology be used to support the actions of "good actors" without aiding "bad actors" as well?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What is the basis for the protection of freedom of expression in the United States, and what types of expressions are not protected under the law?
2. What are some key federal laws that affect online freedom of expression, and how do they impact organizations?
3. What important freedom of expression issues relate to the use of information technology?

FIRST AMENDMENT RIGHTS

The Internet enables a worldwide exchange of news, ideas, opinions, rumors, and information. Its broad accessibility, open discussions, and anonymity make the Internet a remarkable communications medium. It provides an easy and inexpensive way for a speaker to send a message to a large audience—potentially thousands or millions of people worldwide. In addition, given the right email addresses, a speaker can aim a message with laser accuracy at a select subset of powerful and influential people.

People must often make ethical decisions about how to use such incredible freedom and power. Organizations and governments have attempted to establish policies and laws to help guide people, as well as to protect their own interests. Businesses, in particular, have sought to conserve corporate network capacity, avoid legal liability, and improve worker productivity by limiting the nonbusiness use of IT resources.

The right to freedom of expression is one of the most important rights for free people everywhere. The **First Amendment** to the U.S. Constitution (shown in Figure 5-1) was

Kasia/Shutterstock.com

FIGURE 5-1 The U.S. Constitution

adopted to guarantee this right and others. Over the years, a number of federal, state, and local laws have been found unconstitutional because they violated one of the tenets of this amendment.

The First Amendment reads as follows:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

In other words, the First Amendment protects Americans' rights to freedom of religion, freedom of expression, and freedom to assemble peaceably. This amendment has been interpreted by the Supreme Court as applying to the entire federal government, even though it only expressly refers to Congress.

Numerous court decisions have broadened the definition of speech to include nonverbal, visual, and symbolic forms of expression, such as flag burning, dance movements, and hand gestures. Sometimes the speech at issue is unpopular or highly offensive to a majority of people; however, the Bill of Rights provides protection for minority views. The Supreme Court has also ruled that the First Amendment protects the right to speak anonymously as part of the guarantee of free speech.

The Supreme Court has held that the following types of speech are not protected by the First Amendment and may be forbidden by the government: perjury, fraud, defamation, obscene speech, incitement of panic, incitement to crime, "fighting words," and sedition (incitement of discontent or rebellion against a government). Two of these types of speech—obscene speech and defamation—are particularly relevant to information technology.

Obscene Speech

Miller v. California is the 1973 Supreme Court case that established a test to determine if material is obscene and therefore not protected by the First Amendment. After conducting a mass mailing campaign to advertise the sale of adult material, Marvin Miller was convicted of violating a California statute prohibiting the distribution of obscene material. Some unwilling recipients of Miller's brochures complained to the police, initiating the legal proceedings. Although the brochures contained some descriptive printed material, they primarily consisted of pictures and drawings explicitly depicting men and women engaged in sexual activity. In ruling against Miller, the Supreme Court determined that speech can be considered obscene and not protected under the First Amendment based on the following three questions:

- Would the average person, applying contemporary community standards, find that the work, taken as a whole, appeals to the prurient interest?
- Does the work depict or describe, in a patently offensive way, sexual conduct specifically defined by the applicable state law?
- Does the work, taken as a whole, lack serious literary, artistic, political, or scientific value?

These three tests have become the U.S. standard for determining whether something is obscene. The requirement that a work be assessed by its impact on an average adult in a community has raised many questions:

- Who is an average adult?
- What are contemporary community standards?
- What is a community? (This question is particularly relevant in cases in which potentially obscene material is displayed worldwide via the Internet.)

Defamation

The right to freedom of expression is restricted when the expressions, whether spoken or written, are untrue and cause harm to another person. Making either an oral or a written statement of alleged fact that is false and that harms another person is **defamation**. The harm is often of a financial nature, in that it reduces a person's ability to earn a living, work in a profession, or run for an elected office, for example. An oral defamatory statement is **slander**, and a written defamatory statement is **libel**. Because defamation is defined as an untrue statement of fact, truth is an absolute defense against a charge of defamation. Although people have the right to express opinions, they must exercise care in their online communications to avoid possible charges of defamation. Organizations must also be on their guard and be prepared to take action in the event of libelous attacks against them.

A woman sued Gawker Media (a controversial, now-defunct, website that trafficked in news, gossip, and opinion) and its founder for defamation and invasion of privacy. She claimed that a Gawker's blog post speculating that she was dating her boss at tech company Yahoo damaged her reputation and caused her to suffer personally and professionally by stating that she did not conduct herself professionally and ethically and exercised poor judgment in her senior position in the firm's human resources organization.[3]

CRITICAL THINKING EXERCISE: POSTING A NEGATIVE REVIEW ON YELP

Your friend recently had an unpleasant experience at a local eatery where the service was poor and the food overpriced. In addition, she became ill with severe stomach cramps within hours of eating at the restaurant. She has drafted a scathing review and plans to post it on Yelp, accusing the restaurant of giving her food poisoning. She has asked you to look over her review before posting it. What would you say?

FREEDOM OF EXPRESSION: KEY ISSUES

Information technology has provided amazing new ways for people to communicate with others around the world, but with these new methods come new responsibilities and new ethical dilemmas. This section discusses a number of key issues related to the freedom of expression, including controlling access to information on the Internet, Internet censorship, SLAPP lawsuits, anonymity on the Internet, John Doe lawsuits, hate speech, pornography on the Internet, and fake news reporting.

Controlling Access to Information on the Internet

Although there are clear and convincing arguments to support freedom of speech online, the issue is complicated by the ease with which children can access the Internet. Even some advocates of free speech acknowledge the need to restrict children's Internet access, but it is difficult to restrict their access without also restricting adults' access. In attempts to address this issue, the U.S. government has passed laws, and software manufacturers have invented special software to block access to objectionable material. The following sections summarize these approaches.

Communications Decency Act

The Telecommunications Act (Public Law 104-104) became law in 1996. Its primary purpose was to allow free competition among phone, cable, and TV companies. The act was broken into seven major sections or titles. Title V of the Telecommunications Act was the **Communications Decency Act (CDA)**, aimed at protecting children from pornography. The CDA imposed $250,000 fines and prison terms of up to two years for the transmission of "indecent" material over the Internet.

In February 1996, the American Civil Liberties Union (ACLU) and 18 other organizations filed a lawsuit challenging the criminalization of so-called indecency on the web under the CDA. The problem with the CDA was its broad language and vague definition of *indecency*, a standard that was left to individual communities to determine. In June 1997, the Supreme Court ruled the law unconstitutional and declared that the Internet must be afforded the highest protection available under the First Amendment.[4] The Supreme Court said in its ruling that "the interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship."[5] The ruling applied essentially the same free-speech protections to communication over the Internet as exist for print communication.

If the CDA had been judged constitutional, it would have opened all aspects of online content to legal scrutiny. Many current websites would probably either not exist or would look much different today had the law not been overturned. Websites that might have been deemed indecent under the CDA would be operating under an extreme risk of liability.

Section 230 of the CDA, which was not ruled unconstitutional, states that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" (47 U.S.C. § 230). This provides immunity to an Internet service provider (ISP) that publishes user-generated content, as long as its actions do not rise to the level of a content provider. In general, the closer an ISP is to a pure service provider than to a content provider, the more likely that the Section 230 immunity will apply.[6] This portion of the CDA protects social networking companies such as Facebook and Twitter from defamation suits in connection with user postings that appear on their sites.

Facebook presents a constantly updated list of stories, called the News Feed, in the middle of each Facebook user's home page. Using an algorithm based on each user's Facebook activity and connections, the social networking site attempts to choose the "best" content out of several thousand potential stories, placing those near the top of the News

Feed. The number of comments and likes a post receives, as well as what type of story it is (e.g., photo, video, news article, or status update), influences whether and how prominently a story will appear in a user's News Feed. Facebook also conducts surveys and focus groups to get input on what stories people think should appear. The more engaging the content, the more time users will spend on Facebook and the more often they will likely return to the site. This enables Facebook to earn more revenue from ads shown in News Feed content.[7]

Because one of the traditional roles of a publisher is to select which stories to show its readers, Facebook's efforts to shape the news that its users see could result in it being viewed as an information content provider by the courts, resulting in a loss of protection under Section 230 of the CDA. If that were to happen, Facebook could become liable for defamation based on the postings of its subscribers.

Child Online Protection Act

In October 1998, the **Child Online Protection Act (COPA)** was signed into law. This act is not to be confused with the Children's Online Privacy Protection Act (COPPA) that is directed at websites that want to gather personal information from children under the age of 13. COPA states that "whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than $50,000, imprisoned not more than 6 months, or both."[8]

After its passage, COPA became a rallying point for proponents of free speech. Not only could it affect sellers of explicit material online and their potential customers, but it could ultimately set standards for Internet free speech. Supporters of COPA (primarily the Department of Justice) argued that the act protected children from online pornography while preserving the rights of adults. However, privacy advocacy groups—such as the Electronic Privacy Information Center, the ACLU, and the Electronic Frontier Foundation (EFF)—claimed that the language was overly vague and limited the ability of adults to access material protected under the First Amendment.

Following a temporary injunction as well as numerous hearings and appeals, in June 2004 the Supreme Court ruled in *Ashcroft v. American Civil Liberties Union* that there would be "a potential for extraordinary harm and a serious chill upon protected speech" if the law went into effect.[9] The ruling made it clear that COPA was unconstitutional and could not be used to shelter children from online pornography.

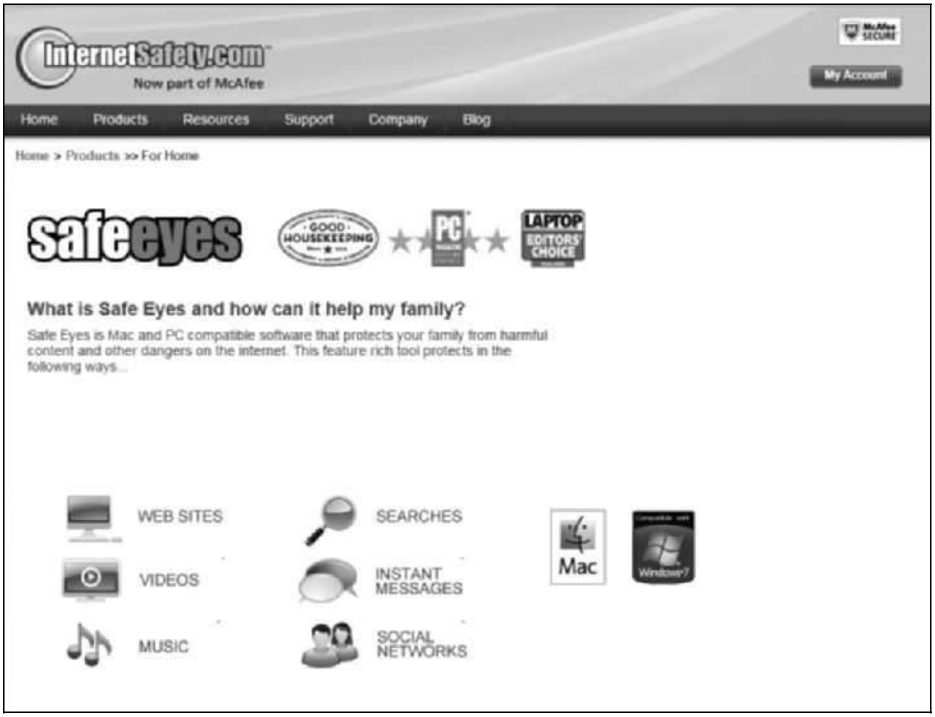
Internet Filtering

An **Internet filter** is software that can be used to block access to certain websites that contain material deemed inappropriate or offensive. The best Internet filters use a combination of URL, keyword, and dynamic content filtering. With URL filtering, a particular URL or domain name is identified as belonging to an objectionable site, and the user is not allowed access to it. Keyword filtering uses keywords or phrases—such as *sex*, *Satan*, and *gambling*—to block websites. With dynamic content filtering, each website's content is evaluated immediately before it is displayed, using techniques such as object analysis and image recognition.

The negative side of Internet filters is that they can block too much content, keeping users from accessing useful information about civil rights, health, sex, and politics as well as online databases and online book catalogs.

Some organizations choose to install filters on their employees' computers to prevent them from viewing sites that contain pornography or other objectionable material. Employees unwillingly exposed to such material would have a strong case for sexual harassment. The use of filters can also ensure that employees do not waste their time viewing nonbusiness-related websites.

According to TopTenREVIEWS, the top rated Internet filters for home users for 2016 include Net Nanny, SpyAgent, and Qustodio.[10] Safe Eyes from InternetSafety.com is an Internet-filtering software that filters videos on YouTube, manages the viewing of online TV using age-appropriate ratings (e.g., TV-G and TV-PG), and blocks the use of media-sharing applications used to download pirated music and videos (see Figure 5-2). Internet software filters have also been developed to run on mobile devices such as Android, iPhone, and Microsoft smartphones.



What is Safe Eyes and how can it help my family?

Safe Eyes is Mac and PC compatible software that protects your family from harmful content and other dangers on the internet. This feature rich tool protects in the following ways...

FIGURE 5-2 Screenshot of Safe Eyes from Internet Safety

Source: InternetSafety.com, part of McAfee Inc.

Another approach to restricting access to websites is to subscribe to an ISP that performs the blocking. The blocking occurs through the ISP's server rather than via software loaded onto each user's computer, so users need not update their software. One such ISP, ClearSail/Family.NET, prevents access to known websites that address such topics as bomb making, gambling, hacking, hate, illegal drugs, pornography, profanity, public chat, satanic activities, and suicide. ClearSail employees search the web daily to uncover new sites to add to ClearSail's block list. The ISP blocks specific URLs and known pornographic-hosting services, as well as other sites based on certain keywords. ClearSail's filtering blocks millions of web pages. Newsgroups are also blocked because of the potential for pornography within them.[11]

Children's Internet Protection Act

In another attempt to protect children from accessing pornography and other explicit material online, Congress passed the **Children's Internet Protection Act (CIPA)** in 2000. The act required federally financed schools and libraries to use some form of technological protection (such as an Internet filter) to block computer access to obscene material, pornography, and anything else considered harmful to minors. Congress did not specifically define what content or websites should be forbidden or what measures should be used—these decisions were left to individual school districts and library systems. Any school or library that failed to comply with the law would no longer be eligible to receive federal money through the E-Rate program, which provides funding to help pay for the cost of Internet connections. The following points summarize CIPA:

- Under CIPA, schools and libraries subject to CIPA will not receive the discounts offered by the E-Rate program unless they certify that they have certain Internet safety measures in place to block or filter pictures that are obscene, contain child pornography, or are harmful to minors (for computers used by minors).
- Schools subject to CIPA are required to adopt a policy to monitor the online activities of minors.
- Schools and libraries subject to CIPA are required to adopt a policy addressing access by minors to inappropriate matter online; the safety and security of minors when using email, chat rooms, and other forms of direct electronic communications; unauthorized access, including hacking and other unlawful activities by minors online; unauthorized disclosure, use, and dissemination of personal information regarding minors; and restricting minors' access to materials harmful to them. CIPA does not require the tracking of Internet use by minors or adults.[12]

Opponents of the law were concerned that it transferred power over education to private software companies who develop the Internet filters and define what sites to block. Furthermore, opponents felt that the motives of these companies were unclear—for example, some filtering companies track students' online activities and sell the data to market research firms. Opponents also pointed out that some versions of these filters were ineffective, blocking access to legitimate sites and allowing access to objectionable ones. Yet another objection was that penalties associated with the act could cause schools and libraries to lose federal funds from the E-Rate program, which is intended to help bridge the digital divide between rich and poor, urban and rural. Loss of federal funds would lead to a less capable version of the Internet for students at poorer schools, which have the fewest alternatives to federal aid.

CIPA's proponents contended that shielding children from drugs, hate speech, pornography, and other topics was a sufficient reason to justify filters. They argued that

Internet filters are highly flexible and customizable and that critics exaggerated the limitations. Proponents pointed out that schools and libraries could elect not to implement a children's Internet protection program; they just wouldn't receive federal money for Internet access.

Many school districts implemented programs consistent with CIPA. Acceptance of an Internet filtering system is more meaningful if the system and its rationale are first discussed with parents, students, teachers, and administrators. Then the program can be refined, taking into account everyone's feedback. An essential element of a successful program is to require that students, parents, and employees sign an agreement outlining the school district's acceptable-use policies for accessing the Internet. Controlling Internet access via a central district-wide network rather than having each school set up its own filtering system reduces administrative effort and ensures consistency. Procedures must be defined to block new objectionable sites as well as remove blocks from websites that should be accessible.

Implementing CIPA in libraries is much more difficult because a library's services are open to people of all ages, including adults who have First Amendment rights to access a broader range of online materials than are allowed under CIPA. In *United States, et al. v. American Library Association, Inc., et al.*, the American Library Association challenged CIPA. Ultimately in that case, the Supreme Court made it clear that the constitutionality of government-mandated filtering schemes depends on adult patrons' ability to request and receive unrestricted access to protected speech.[13] A possible compromise for public libraries with multiple computers would be to allow unrestricted Internet use for adults but to provide computers with only limited access for children.

Rather than deal with all the technical and legal complications, some librarians say they wish they could simply focus on training students and adults to use the Internet safely and wisely.

Digital Millennium Copyright Act

The **Digital Millennium Copyright Act (DMCA)**, which was signed into law in 1998, addresses a number of copyright-related issues. The DMCA is divided into five titles that will be discussed more fully in Chapter 6. Title II, the "Online Copyright Infringement Liability Limitation Act," provides limitations on the liability of an ISP for copyright infringement that can arise when an ISP subscriber posts copyrighted material such as audio tracks, videos, books, and news articles on the Internet. Its passage amended Title 17 of the U.S. Code (Copyright) by adding a new Section 512, which says that an ISP cannot be held liable for copyright infringement if, when notified by the copyright holder, it notifies the subscriber of the alleged infringement and executes a "takedown" by removing the offending content.[14] The fact that the content was created by you, or in the case of a photo or video the subject is you, can be sufficient enough to request a takedown.

A woman posted a 29-second video on YouTube of her baby dancing in the kitchen with Prince's "Let's Go Crazy" playing in the background. Universal Music Corporation sent YouTube a DMCA takedown notice claiming use of its song constituted copyright infringement. The video was initially removed from YouTube for a few weeks but was eventually reinstated. The case has been in the courts for over seven years and has raised the issue that copyright owners need to consider fair use before they issue a DMCA takedown notice. (Fair use is the copying of copyrighted material done for a limited and "transformative" purpose, such as to comment upon, criticize, or parody a copyrighted work. Fair use can be done without permission from the copyright owner and is a defense against copyright infringement).[15]

Internet Censorship

Internet censorship is the control or suppression of the publishing or accessing of information on the Internet. Speech on the Internet requires a series of intermediaries to reach its audience (see Figure 5-3) with each intermediary vulnerable to some degree of pressure from those who want to silence the speaker. Web hosting services are often the recipients of defamation or copyright infringement claims by government authorities or copyright holders, demanding the immediate takedown of hosted material that is deemed inappropriate or illegal. Government entities may pressure "upstream" Internet service providers to limit access to certain websites, allow access to only some content or modified content at certain websites, reject the use of certain keywords in search engines, and track and monitor the Internet activities of individuals. Several countries have enacted the so-called three-strikes laws that require ISPs to terminate a user's Internet connection once that user has received a number of notifications of posting of content deemed inappropriate or illegal. Censorship efforts may also focus on Domain Name System (DNS) servers, which convert human-readable host and domain names into the machine-readable, numeric Internet Protocol (IP) addresses that are used to point computers and other devices toward the correct servers on the Internet. Where authorities have control over DNS servers, officials can "deregister" a domain that hosts content that is deemed inappropriate or illegal so that the website is effectively invisible to users seeking access to the site.

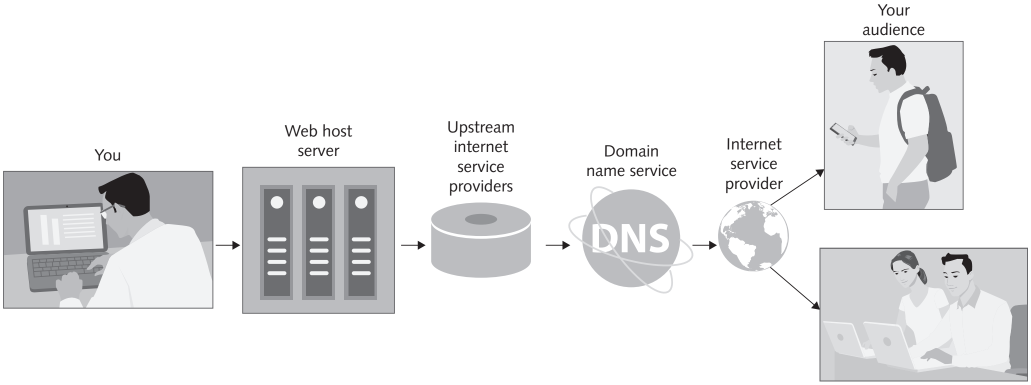

You
Web host server
Upstream internet service providers
Domain name service
DNS
Internet service provider
Your audience

FIGURE 5-3 Internet Censorship

China has the largest online population in the world, with over 721 million Internet users (see Table 5-1, which depicts the top 10 countries in terms of number of Internet users); however, Internet censorship in China is perhaps the most rigorous in the world. The Chinese government blocks access to websites that discuss any of a long list of topics that are considered objectionable—including the Buddhist leader the Dalai Lama, anything to do with the government crackdown on the 1989 Tiananmen Square protests, and the banned spiritual movement Falun Gong. Chinese websites also employ censors who monitor and delete objectionable content. The government even hires workers to post comments favorable to the government.[16]

TABLE 5-1 The top 10 countries with the highest number of Internet users (2016)

Rank	Country	Internet users (millions)	Population (millions)	Penetration (% of population)
1	China	721	1,382	52
2	India	462	1,327	35
3	United States	287	324	89
4	Brazil	139	210	66
5	Japan	115	126	91
6	Russia	102	143	71
7	Nigeria	86	187	46
8	Germany	71	81	88
9	United Kingdom	60	65	93
10	Mexico	58	129	45

Source: Internet Users by Country (2016), *Internet Live Stats*, www.internetlivestats.com/internet-users-by-country.

Brazilian government demands have closed more Google Gmail accounts and more blog sites than in any other country. In Brazil, filing a lawsuit to demand that Internet content be taken down is relatively easy and inexpensive. The ability of litigants to challenge content and demand that anonymous sources be revealed stifles Brazilian journalists and Internet bloggers.[17]

In Cuba, only a few people can afford Internet access; currently, only 5 percent of homes are connected. Although Cuba has said it plans to double access in the next five years, the government continues to engage in censorship activities by frequently filtering and intermittently blocking websites that are critical of the state.[18]

Reporters without Borders (RWB), an international nonprofit, nongovernmental organization with headquarters in Paris, promotes and defends freedom of information and freedom of the press around the world. Each year, RWB prepares an “Enemies of the Internet” list, which includes countries the group has determined have the highest levels of Internet censorship and surveillance. The United States and the United Kingdom were added to the 2014 edition of this list after information leaked by Edward Snowden revealed a high degree of government surveillance in both countries.[19]

Strategic Lawsuit Against Public Participation

A **strategic lawsuit against public participation (SLAPP)** is employed by corporations, government officials, and others against citizens and community groups who oppose them on matters of public interest. The lawsuit is typically without merit and is used to intimidate critics out of fear of the cost and efforts associated with a major legal battle. Many question the ethics and legality of using a SLAPP; others claim that all is fair when it comes to politics and political issues.

Of course, the plaintiff in a SLAPP cannot present themselves to the court admitting that their intent is to censor their critics. Instead, the SLAPP takes some other form, such as a defamation lawsuit that make claims with vague wording that enables plaintiffs to make bogus accusations without fear of perjury. The plaintiff refuses to consider any settlement and initiates an endless stream of appeals and delays in an attempt to drag the suit out and run up the legal costs.[20]

Every year thousands of people become SLAPP victims while participating in perfectly legal actions such as phoning a public official, writing a letter to the editor of a newspaper, speaking out at a public meeting, posting an online review, or circulating a petition.[21] For example, an unhappy home owner wrote two scathing reviews on Yelp when the contractor he had hired to install a new hardwood floor botched the job. For six months, the homeowner and contractor tried to work things out but to no avail. The contractor sued the home owner for civil theft, intentional interference, and defamation claiming the online reviews had caused it to lose $625,000 worth of business and demanded $125,000 in compensation. The home owner eventually removed the reviews, but only after spending $60,000 on legal fees plus another $15,000 to settle the case. The contractor insisted that its suit wasn't a SLAPP because it was filed months after the reviews were posted, was primarily about the homeowner's failure to pay, and involved a legitimate defamation claim.[22]

Anti-SLAPP laws are designed to reduce frivolous SLAPPs. As of 2015, 28 states and the District of Columbia had passed anti-SLAPP legislation to protect people who are the target of a SLAPP.[23] Typically, under such legislation, a person hit with what they deem to be a SLAPP can quickly file an anti-SLAPP motion, which puts a hold on the original lawsuit until the court determines whether the defendant was being targeted for exercising free-speech rights, petitioning the government, or speaking in a public forum on "an issue of public interest." In such cases, the SLAPP lawsuit is thrown out unless the plaintiff can show that the claims are legitimate and likely to succeed at trial. To guard against abusive anti-SLAPP motions, the side that loses such a case is required to pay the other side's legal fees.[24]

Anonymity on the Internet

Anonymous expression is the expression of opinions by people who do not reveal their identity. The freedom to express an opinion without fear of reprisal is an important right of a democratic society. Anonymity is even more important in countries that don't allow free speech. However, in the wrong hands, anonymous communication can be used as a tool to commit illegal or unethical activities.

Anonymous political expression played an important role in the early formation of the United States. Before and during the American Revolution, patriots who dissented against British rule often used anonymous pamphlets and leaflets to express their opinions. England had a variety of laws designed to restrict anonymous political commentary, and people found guilty of breaking these laws were subject to harsh punishment—from whippings to hangings. A famous case in 1735 involved a printer named John Zenger, who was prosecuted for seditious libel because he wouldn't reveal the names of anonymous authors whose writings he published. The authors were critical of the governor of New York. The British were outraged when the jurors refused to convict Zenger, in what is considered a defining moment in the history of freedom of the press in the United States.

Other democracy supporters often authored their writings anonymously or under pseudonyms. For example, Thomas Paine was an influential writer, philosopher, and statesman of the Revolutionary War era. He published a pamphlet called *Common Sense*, in which he criticized the British monarchy and urged the colonies to become independent by establishing a republican government of their own. Published anonymously in 1776, the pamphlet sold more than 500,000 copies, at a time when the population of the colonies was estimated to have been less than four million; it provided a stimulus to produce the Declaration of Independence six months later.

Despite the importance of anonymity in early America, it took nearly 200 years for the Supreme Court to render rulings that addressed anonymity as an aspect of the Bill of Rights. One of the first rulings was in the 1958 case of *National Association for the Advancement of Colored People (NAACP) v. Alabama*, in which the court ruled that the NAACP did not have to turn over its membership list to the state of Alabama. The court believed that members could be subjected to threats and retaliation if the list were disclosed and that disclosure would restrict a member's right to freely associate, in violation of the First Amendment.

Another landmark anonymity case involved a sailor threatened with discharge from the U.S. Navy because of information obtained from AOL. In 1998, following a tip, a Navy investigator asked AOL to identify the sailor, who used a pseudonym to post information in an online personal profile that suggested he might be gay. Thus, he could be discharged under the military's "don't ask, don't tell" policy, which was in effect at the time. AOL admitted that its representative violated company policy by providing the information. A federal judge ruled that the Navy had overstepped its authority in investigating the sailor's sexual orientation and had also violated the Electronic Communications Privacy Act, which limits how government agencies can seek information from email or other online data. The sailor received undisclosed monetary damages from AOL and, in a separate agreement, was allowed to retire from the Navy with full pension and benefits.[25]

Doxing involves doing research on the Internet to obtain someone's private personal information—such as home address, email address, phone numbers, and place of employment—and even private electronic documents, such as photographs, and then posting that information online without permission. Doxing may be done as an act of revenge for a perceived slight or as an effort to publicly shame someone who has been operating anonymously online. Sadly, in some cases it is simply done for kicks.

In 2015, an American dentist shot and killed a lion named Cecil in Zimbabwe in a way that likely broke the law. Cecil was quite popular with visitors to the national park where he lived, and people around the world were upset by the news. Shortly after the dentist's identity was released, he became a victim of doxing. The URL for his practice's website and his work address and phone number were posted online and shared repeatedly across a variety of social networks. The dentist had his life threatened online, faced protesters outside his office, and had his vacation home in Florida vandalized.[26]

Maintaining anonymity on the Internet is important to some computer users. They might be seeking help in an online support group, reporting defects about a manufacturer's goods or services, taking part in frank discussions of sensitive topics, expressing a minority or antigovernment opinion in a hostile political environment, or participating in chat rooms. Other Internet users, however, would prefer to ban web anonymity because they think its use increases the risks of defamation and fraud, as well as the exploitation of children.

When an email is sent, the email software (for example, Outlook) automatically inserts information called a header on each packet of the message that identifies where the email originated from and who sent it. In addition, IP addresses are attached to the email and captured as the message transfers through various routers and relay servers. Internet users who want to remain anonymous can send email to an **anonymous remailer service**, which uses a computer program to strip the originating header and/or IP number from the message. It then forwards the message to its intended recipient—an individual, a chat room, or a newsgroup—with either no IP address or a fake one, ensuring that the header information cannot be used to identify the author. Some remailers route messages through multiple remailers to provide a virtually untraceable level of anonymity. Anonymous remailers do not keep any list of users and corresponding anonymizing labels used for them; thus, a remailer can ensure its users that no internal information has been left behind that can later be used to break identity confidentiality. Even if law-enforcement agencies serve a court order to release information, there is nothing to turn over.

The use of a remailer keeps communications anonymous; what is communicated, and whether it is ethical or legal, is up to the sender. The use of remailers by people committing unethical or even illegal acts in some states or countries has spurred controversy. Remailers are frequently used to send pornography, to illegally post copyrighted material to Usenet newsgroups, and to send unsolicited advertising to broad audiences (spamming). An organization's IT department can set up a firewall to prohibit employees from accessing remailers or to send a warning message each time an employee communicates with a remailer.

As part of an antiterrorist operation in late 2014, police in Spain raided 14 houses and social centers. Seven people arrested that day were held in a Madrid prison on suspicion of terrorism. The judge in the case cited three reasons for jailing the seven people—possession of certain books, including *Against Democracy* (a book that challenges the belief that the version of democracy practiced today is good and moral), the production of publications and forms of communication, and their use on an anonymous remailer to send emails. Many privacy experts believe that citing the use of secure email as a potential indicator of involvement in terrorist activities is an exceedingly dangerous precedent. As one blogger commented and many observers agree "Security is not a crime."[27]

John Doe Lawsuits

Businesses must monitor and respond to both the public expression of opinions that might hurt their reputations and the public sharing of confidential company information. When anonymous employees reveal harmful information online, the potential for broad dissemination is enormous, and it can require great effort to identify the people involved and stop them.

An aggrieved party can file a **John Doe lawsuit** against a defendant whose identity is temporarily unknown because he or she is communicating anonymously or using a pseudonym. Once the John Doe lawsuit is filed, the plaintiff can request court permission to issue subpoenas to command a person to appear under penalty. If the court grants permission, the plaintiff can serve subpoenas on any third party—such as an ISP or a website hosting firm—that may have information about the true identity of the defendant. When, and if, the identity becomes known, the complaint is modified to show the correct name(s) of the defendant(s). This approach is also frequently employed in copyright infringement lawsuits where unknown parties have downloaded movies or music from the Internet.

ISPs—such as AT&T, Comcast, and CenturyLink—and social networking sites—such as Facebook and Pinterest—receive more than a thousand subpoenas per year directing them to reveal the identity of John Does. Free-speech advocates argue that if someone charges libel, the anonymity of the web poster should be preserved until the libel is proved. Otherwise, the subpoena power can be used to silence anonymous, critical speech.

Proponents of such lawsuits point out that most John Doe cases are based on serious allegations of wrongdoing, such as libel or disclosure of confidential information. For example, stock price manipulators can use chat rooms to affect the share price of stocks—especially those of very small companies that have just a few outstanding shares. In addition, competitors of an organization might try to create the feeling that the organization is a miserable place to work, which could discourage job candidates from applying, investors from buying stock, or consumers from buying company products. Proponents of John Doe lawsuits argue that perpetrators should not be able to hide behind anonymity to avoid responsibility for their actions.

Anonymity is not guaranteed. By filing a lawsuit, companies gain immediate subpoena power, and many message board hosts release information as soon as it is requested, often without notifying the poster. Everyone who posts comments in a public place on the web should consider the consequences if their identities were to be exposed. Furthermore, everyone who reads anonymous postings online should think twice about believing what they read.

The California State Court in *Pre-Paid Legal v. Sturtz et al.*[28] set a legal precedent that refined the criteria the courts apply when deciding whether or not to approve subpoenas requesting the identity of anonymous web posters. The case involved a subpoena issued by Pre-Paid Legal Services (PPLS), which requested the identity of eight anonymous posters on Yahoo's Prepaid message board. Attorneys for PPLS argued that the company needed the posters' identities to determine whether they were subject to a voluntary injunction that prevented former sales associates from revealing PPLS's trade secrets.

The EFF represented two of the John Does whose identities were subpoenaed. EFF attorneys argued that the message board postings cited by PPLS revealed no company secrets but were merely disparaging the company and its treatment of sales associates. They argued further that requiring the John Does to reveal their identities would let the company punish them for speaking out and set a dangerous precedent that would discourage other Internet users from voicing criticism. Without proper safeguards on John Doe subpoenas, a company could use the courts to uncover its critics.

EFF attorneys urged the court to apply the four-part test adopted by the federal courts in *Doe v. 2TheMart.com, Inc*.[29] to determine whether a subpoena for the identity of the web posters should be upheld. In that case, the federal court ruled that a subpoena should be enforced only when the following occurs:

- The subpoena was issued in good faith and not for any improper purpose.
- The information sought was related to a core claim or defense.
- The identifying information was directly and materially relevant to that claim or defense.
- Adequate information was unavailable from any other source.

A judge in Santa Clara County Superior Court invalidated the subpoena requesting the posters' identities. He ruled that the messages were not obvious violations of the injunctions invoked by PPLS and that the First Amendment protection of anonymous speech outweighed PPLS's interest in learning the identity of the speakers.

Hate Speech

In the United States, speech that is merely annoying, critical, demeaning, or offensive enjoys protection under the First Amendment. Legal recourse is possible only when hate speech turns into clear threats and intimidation against *specific* citizens. Persistent or malicious harassment aimed at a specific person is **hate speech**, which can be prosecuted under the law, but general, broad statements expressing hatred of an ethnic, racial, or religious group cannot. A threatening private message sent over the Internet to a person, a public message displayed on a website describing intent to commit acts of hate-motivated violence against specific individuals, and libel directed at a particular person are all actions that can be prosecuted.

Although ISPs and social networking sites do not have the resources to prescreen content (and they do not assume any responsibility for content provided by others), many ISPs and social networking sites do reserve the right to remove content that, in their judgment, does not meet their standards. The speed at which content may be removed depends on how quickly such content is called to the attention of the ISP or social networking site, how egregious the content is, and the general availability of the company's resources to handle such issues.

To post videos on YouTube, you must first create a YouTube or a Google account (Google is the owner of YouTube) and agree to abide by the site's published guidelines.[30] The YouTube guidelines prohibit the posting of videos showing such things as pornography, animal abuse, graphic violence, predatory behavior, and drug use. The guidelines also prohibit the posting of copyrighted material—such as music, television programs, or movies—that is owned by a third party. YouTube staff members review user-posted videos on a regular basis to find any that violate the site's community guidelines. Those that violate the guidelines are removed. Certain other videos are age-restricted because of their content. Users are penalized for serious or repeated violations of the guidelines and can have their account terminated.[31]

Because such prohibitions are included in the service contracts between ISPs and social networking sites and their subscribers and members—and do not involve the federal government—they do not violate anyone's First Amendment rights. Of course, people who lose an ISP or social networking account for violating the provider's regulations may resume their hate speech by simply opening a new account, either under a different name or with some other, more permissive site or ISP.

Gerardo Ortiz is an American regional Mexican singer-songwriter and record producer whose "Fuiste Mía" music video depicts him tossing his girlfriend into the trunk of his car and setting the car on fire after catching her with another man. The video was removed from YouTube following an online petition with over 6,000 signatures demanding the video be taken down for promoting and inciting violence against women. Ortiz defended the video as pure fiction where no one was actually harmed and compared it to content seen in movies and TV shows, but personally made the decision to have the video taken down at least temporarily.[32] The video raises questions of artistic liberty and freedom of speech.[33]

Although they may implement a speech code, public schools and universities are legally considered agents of the government and therefore must follow the First Amendment's prohibition against speech restrictions based on content or viewpoint. Corporations, private schools, and private universities, on the other hand, are not part of state or federal government. As a result, they may prohibit students, instructors, and other employees from engaging in offensive speech using corporate-, school-, or university-owned computers, networks, or email services.

Most other countries do not provide constitutional protection for hate speech. For example, promoting Nazi ideology is a crime in Germany, and denying the occurrence of the Holocaust is illegal in many European countries. Authorities in Britain, Canada, Denmark, France, and Germany have charged people for crimes involving hate speech on the web.

A U.S. citizen who posts material on the web that is illegal in a foreign country can be prosecuted if the person subjects himself or herself to the jurisdiction of that country—for example, by visiting there. As long as the person remains in the United States, that person is safe from prosecution because U.S. laws do not allow a person to be extradited for engaging in an activity protected by the U.S. Constitution, even if the activity violates the criminal laws of another country.

Pornography on the Internet

Many people, including some free-speech advocates, believe that there is nothing illegal or wrong about purchasing adult pornographic material made by and for consenting adults. They argue that the First Amendment protects such material. On the other hand, most parents, educators, and other child advocates are concerned that children might be exposed to online pornography. They are deeply troubled by its potential impact on children and fear that increasingly easy access to pornography encourages pedophiles and sexual predators.

Clearly, the Internet has been a boon to the pornography industry by providing fast, cheap, and convenient access to many millions of porn websites worldwide.[34] Access via the Internet enables pornography consumers to avoid offending others or being embarrassed by others observing their purchases. There is no question that online adult pornography is big business (revenue estimates vary widely between $1 billion and $97 billion) and generates a lot of traffic; it is estimated that there are over 72 million visitors to pornographic websites monthly.[35,36]

If what someone distributes or exhibits is judged obscene, they are subject to prosecution under the obscenity laws. The precedent-setting *Miller v. California* ruling on obscenity discussed earlier in the chapter predates the Internet. The judges in that case ruled that contemporary community standards should be used to judge what is obscene. The judges allowed that different communities could have different norms.

The key question in deciding what Internet material is obscene is: "Whose community standards are used?" Because Internet content publishers cannot easily direct their content into or away from a particular geographic area, one answer to this question is that the Internet content publisher must conform to the norms of the most restrictive community. However, this line of reasoning was challenged by the Third Circuit Court of Appeals in the *Ashcroft v. American Civil Liberties Union* case, which involved a challenge to the 1998 COPA. The Supreme Court reversed the circuit court's ruling in this case—but with five different opinions and no clear consensus on the use of local or national community standards.[37] In *United States v. Kilbride*, the Ninth Circuit Court of Appeals ruled that "a national community standard must be applied in regulating obscene speech on the Internet, including obscenity disseminated via email."[38] In *United States v. Little*, the Eleventh Circuit Court of Appeals rejected the national community standard and adopted the older, local community standard. Currently, there is no clear agreement within the courts on whether local or national community standards are to be used to judge obscenity.

U.S. organizations must be very careful when dealing with issues relating to pornography in the workplace. By providing computers, Internet access, and training in how to use those computers and the Internet, companies could be seen by the law as purveyors of pornography because they have enabled employees to store pornographic material and retrieve it on demand. Nielsen has found that 25 percent of working adults admit to looking at pornography on a computer at work.[39] In addition, if an employee sees a coworker viewing porn on a workplace computer, that employee may be able to claim that the company has created a hostile work environment. Such a claim opens the organization to a sexual harassment lawsuit that can cost hundreds of thousands of dollars and tie up managers and executives in endless depositions and court appearances.

Many companies believe that they have a duty to stop the viewing of pornography in the workplace. As long as they can show that they took reasonable steps and determined actions to prevent it, they have a valid defense if they become the subject of a sexual harassment lawsuit. If it can be shown that a company made only a half-hearted attempt to stop the viewing of pornography in the workplace, then the company could have trouble defending itself in court. Reasonable steps include establishing and communicating an acceptable use policy that prohibits access to pornography sites, identifying those who violate the policy, and taking disciplinary action against those who violate the policy, up to and including termination.

A few companies take the opposite viewpoint—that they cannot be held liable if they don't know employees are viewing, downloading, and distributing pornography. Therefore, they believe the best approach is to ignore the problem by never investigating it, thereby ensuring that they can claim that they never knew it was happening. Many people would consider such an approach unethical and would view management as shirking an important responsibility to provide a work environment free of sexual harassment. Employees unwillingly exposed to pornography would have a strong case for sexual harassment because they could claim that pornographic material was available in the workplace and that the company took inadequate measures to control the situation.

Numerous federal laws address issues related to child pornography—including laws concerning the possession, production, distribution, or sale of pornographic images or videos that exploit or display children. Possession of child pornography is a federal offense punishable by up to five years in prison. The production and distribution of such materials carry harsher penalties; decades or even life in prison is not an unusual sentence. In addition to these federal statutes, all states have enacted laws against the production and distribution of child pornography, and all but a few states have outlawed the possession of child pornography. At least seven states have passed laws that require computer technicians who discover child pornography on clients' computers to report it to law enforcement officials.

Sexting—sending sexual messages, nude or seminude photos, or sexually explicit videos over a cell phone—is a fast-growing trend among teens and young adults. A Drexel University survey of college students revealed that 54 percent had sent or received "sexually explicit text messages or images" when they were under age 18. Previous studies had pegged the number much lower—around 20 percent. Students in this study may have been more honest because they were allowed to remain anonymous and were reporting on past behavior.[40]

Increasingly, people who take part in sexting are suffering the consequences of this fad. Once an image or video is sent, there is no taking it back and no telling to whom it might be forwarded. And it is not just teenagers who participate in sexting. Consider quarterback Bret Favre and U.S. representative Anthony Weiner who were both parties to embarrassing sexting episodes. Sexters can also face prosecution for child pornography, leading to possible years in jail and decades of registration as a sex offender. Some states have adopted laws that prescribe penalties aimed specifically at teenagers engaged in sexting. These laws make the penalties for teen sexting less severe than if an adult would send similar photos to an under-age person.

Controlling the Assault of Non-Solicited Pornography and Marketing Act

The **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act** (15 U.S.C. § 7704) specifies requirements that commercial emailers must follow when sending messages that have a primary purpose to advertise or promote a commercial product or service. The key requirements of the law include:

- The *From* and *To* fields in the email, as well as the originating domain name and email address, must be accurate and identify the person who initiated the email.
- The subject line of the email cannot mislead the recipient as to the contents or subject matter of the message. In addition, if the message contains sexually oriented material, the phrase "SEXUALLY EXPLICIT" must appear in capital letters as the first characters in the subject line.
- The email must be identified as an advertisement and include a valid physical postal address for the sender.
- The emailer must provide a return email address or some other Internet-based response procedure to enable the recipient to request no future emails, and the emailer must honor such requests to opt out.
- The emailer has 10 days to honor the opt-out request.

- Additional rules prohibit the harvesting of email addresses from websites, using automated methods to register for multiple email accounts, or relaying email through another computer without the owner's permission.

Messages whose primary purpose is to communicate information about a specific transaction or relationship between the sender and recipient are not subject to the CAN-SPAM Act. Thus, a message regarding an attempt to deliver a legitimately placed online order or information about a product recall would be exempt.

Each violation of the provisions of the CAN-SPAM Act can result in a fine of up to $250 for each unsolicited email, and fines can be tripled in certain cases. A Canadian spammer was ordered to pay $873 million in fines for allegedly spamming Facebook accounts with over four million posts. Of course, the spammer could not pay the fine and instead declared bankruptcy.[41]

The Federal Trade Commission (FTC) is charged with enforcing the CAN-SPAM Act, and the agency maintains a consumer complaint database relating to the law. Consumers can submit complaints online at *www.ftc.gov* or forward email to the FTC at *spam@use.gov*. Other countries have their own version of the CAN-SPAM Act.

The CAN-SPAM Act can also be used in the fight against the dissemination of pornography. For example, two men were indicted by an Arizona grand jury for violating the CAN-SPAM Act by sending massive amounts of unsolicited email advertising pornographic websites. They had amassed an email database of 43 million people and used it to send emails containing pornographic images. AOL stated it received over 660,000 complaints from people who received spam from the two, whose operation was highly profitable—enabling the two men to earn over $1.4 million in 2003. The defendants ran afoul of the CAN-SPAM Act by sending messages with false return addresses and for using domain names registered using false information. They were convicted of multiple counts of spamming and criminal conspiracy, which carry a maximum sentence of five years each plus a fine of $500,000 and up to 20 years for money laundering. This is believed to be the first conviction involving CAN-SPAM Act violations.[42] A man nicknamed the Spam King was sentenced to 2½ years in prison and fined $310,000 for sending some 27 million spam emails to Facebook users. He was not prosecuted under the CAN-SPAM Act but instead was found guilty of federal charges including fraud and criminal contempt in connection with using electronic mail.[43]

There is considerable debate over whether the CAN-SPAM Act has helped control the growth of spam. After all, the act clearly defines the conditions under which the sending of spam is legal, and as long as mass emailers meet these requirements, they cannot be prosecuted. Some suggest that the act could be improved by penalizing the companies that use spam to advertise, as well as ISPs who support the spammers.

Fake News

Journalism, including the ways in which people get their news, is going through a period of rapid change. The sale of traditional newspapers and magazines continues to fall while online consumption of news is growing. Nearly twice as many adults (38 percent) report that they often get news online rather than from print media (20 percent).[44] Much online news continues to come from traditional news sources, such as ABC, CBS, CNN, Fox, and NBC news, the *Chicago Tribune*, the *New York Times*, *Newsweek*, the *Wall Street Journal*, and *U.S. News & World Report*. However, readers looking for news and information online will also find a wide range of nontraditional sources—some of which offer more objective, verifiable news reporting than others—including the following types:

- Blogs—On some blogs, writers discuss news and editorial content produced by other journalists and encourage reader participation. Bloggers often report on things about which they are very passionate. As a result, they may be less likely to remain unbiased, instead stating their opinion and supporting facts without presenting the other side of an argument. Indeed, many bloggers pride themselves on their lack of objectivity, instead viewing themselves as an activist for a particular cause or point of view.
- Fake news sites—These sites attempt to imitate real news sites, often modifying real news stories in such a way as to entice viewers into clicking on them. In other cases, fake news sites simply create entirely fictitious "news" stories and present them as fact. In many cases, readers of online news simply glance at headlines or skim an article without ever realizing it is fake or distorted news. Indeed, almost a quarter of Americans admit to sharing fake news, and about two-thirds say that fake news has caused "a great deal of confusion" about current events.
- Social media sites—Ordinary citizens are increasingly involved in the collection, reporting, analysis, and dissemination of news, opinions, and photos, which are then posted to various social media sites. Often, citizen journalists are "on the spot" and able to report on breaking news stories before traditional news reporters. While such timeliness of reporting can be a good thing, it does not always promote accuracy, clarity, and objectivity. Because reports, images, opinions, and videos shared via social media often spread like wildfire, they can sometimes cause confusion, misunderstanding, and controversy, rather than bringing clarity to a situation.

The proliferation of online sources of information and opinion means that the Internet is full of "news" accounts that are, in fact, highly opinionated, fictionalized, or satirical accounts of current events presented in journalistic style. Headlines from such "fake news" stories in 2016 include "Pope Francis shocks world, endorses Donald Trump for president," "WikiLeaks confirms Hillary sold weapons to ISIS," and "FBI agent suspected in Hillary email leaks found dead in apparent murder-suicide." Critics of such sites argue that real journalists adhere to certain standards, such as fact checking, identifying and verifying sources, presenting opinions on both sides of an issue, and avoiding libelous statements. While there are many legitimate online journalists who produce high-quality, evidence-based reporting, too often, online reporting stresses immediacy, speed, sensationalism, and the need for post-publication correction.

Table 5-2 provides a manager's checklist for dealing with issues of freedom of expression in the workplace. In each case, the preferred answer is *yes*.

TABLE 5-2 Manager's checklist for handling freedom of expression issues in the workplace

Question	Yes	No
Do you have a written data privacy policy that is followed?		
Does your corporate IT usage policy discuss the need to conserve corporate network capacity, avoid legal liability, and improve worker productivity by limiting the nonbusiness use of information resources?		
Did the developers of your policy consider the need to limit employee access to nonbusiness-related websites (e.g., Internet filters, firewall configurations, or the use of an ISP that blocks access to such sites)?		
Does your corporate IT usage policy discuss the inappropriate use of anonymous remailers?		
Has your corporate firewall been set to detect the use of anonymous remailers?		
Has your company (in cooperation with legal counsel) formed a policy on the use of John Doe lawsuits to identify the authors of libelous, anonymous email?		
Does your corporate IT usage policy make it clear that defamation and hate speech have no place in the business setting?		
Does your corporate IT usage policy prohibit the viewing and sending of pornography?		
Does your corporate acceptable use policy communicate that employee email is regularly monitored for defamatory, hateful, and pornographic material?		
Does your corporate IT usage policy tell employees what to do if they receive hate mail or pornography?		

CRITICAL THINKING EXERCISE: FILING A JOHN DOE LAWSUIT

You are a young, recently graduated attorney working part-time as part of the re-election campaign team for your midsized city's mayor. Several citizens have taken to writing strongly worded anonymous letters to the local newspaper voicing their disagreement over your candidate's actions in her initial term as mayor. The campaign manager has suggested that you file John Doe lawsuits against the most vocal complainers as a warning to others of what they can expect if they are too vocal in their disagreement with the mayor. The goal is to intimidate others who might be inclined to write negative letters to the newspaper. Do you think this tactic will be successful? Why or why not?

Summary

What is the basis for the protection of freedom of expression in the United States, and what types of expressions are not protected under the law?

- The First Amendment protects Americans' rights to freedom of religion, freedom of expression, and freedom to assemble peaceably. The Supreme Court has ruled that the First Amendment also protects the right to speak anonymously.
- Obscene speech, defamation, incitement of panic, incitement to crime, "fighting words," and sedition are not protected by the First Amendment and may be forbidden by the government.

What are some key federal laws that affect online freedom of expression, and how do they impact organizations?

- Although there are clear and convincing arguments to support freedom of speech on the Internet, the issue is complicated by the ease with which children can use the Internet to gain access to material that many parents and others feel is inappropriate for children. The conundrum is that it is difficult to restrict children's Internet access without also restricting adults' access.
- The U.S. government has passed several laws to attempt to address this issue, including the Communications Decency Act (CDA), which is aimed at protecting children from online pornography, and the Child Online Protection Act (COPA), which prohibits making harmful material available to minors via the Internet. Both laws were ultimately ruled largely unconstitutional. However, Section 230 of the CDA, which was not ruled unconstitutional, provides immunity from defamation charges to ISPs that publish user-generated content, as long as they do not also serve as a content provider.
- Software manufacturers have developed Internet filters, which are designed to block access to objectionable material through a combination of URL, keyword, and dynamic content filtering.
- The Children's Internet Protection Act (CIPA) requires federally financed schools and libraries to use filters to block computer access to any material considered harmful to minors. In *United States v. American Library Association, Inc.*, the American Library Association challenged CIPA. Ultimately in that case, the Supreme Court made it clear that the constitutionality of government-mandated filtering schemes depends on adult patrons' ability to request and receive unrestricted access to protected speech.
- The Digital Millennium Copyright Act (DMCA) addresses a number of copyright-related issues, with Title II of the act providing limitations on the liability of an ISP for copyright infringement.

What important freedom of expression issues relate to the use of information technology?

- Internet censorship is the control or suppression of the publishing or accessing of information on the Internet. There are many forms of Internet censorship. Many countries practice some form of Internet censorship.
- A SLAPP (strategic lawsuit against public participation) is a lawsuit filed by corporations, government officials, and others against citizens and community groups who oppose them on matters of concern. Anti-SLAPP laws are designed to reduce frivolous SLAPPs. As of

2015, 28 states and the District of Columbia have put into effect anti-SLAPP legislation to protect people who are the target of a SLAPP.

- Anonymous expression is the expression of opinions by people who do not reveal their identity. The freedom to express an opinion without fear of reprisal is an important right of a democratic society. Anonymity is even more important in countries that don't allow free speech. Maintaining anonymity on the Internet is important to some computer users. Such users sometimes use an anonymous remailer service, which strips the originating header and/or IP address from the message and then forwards the message to its intended recipient.
- Doxing involves doing research on the Internet to obtain someone's private personal information (such as home address, email address, phone numbers, and place of employment) and even private electronic documents (such as photographs), and then posting that information online without permission.
- Many businesses monitor the web for the public expression of opinions that might hurt their reputations. They also try to guard against the public sharing of company confidential information.
- Organizations may file a John Doe lawsuit to enable them to gain subpoena power in an effort to learn the identity of anonymous Internet users who they believe have caused some form of harm to the organization through their postings.
- In the United States, speech that is merely annoying, critical, demeaning, or offensive enjoys protection under the First Amendment. Legal recourse is possible only when hate speech turns into clear threats and intimidation against specific citizens.
- Some ISPs and social networking sites have voluntarily agreed to prohibit their subscribers and members from sending hate messages using their services. Because such prohibitions can be included in the service contracts between a private ISP and its subscribers or a social networking site and it members—and do not involve the federal government—they do not violate subscribers' First Amendment rights.
- Many adults, including some free-speech advocates, believe there is nothing illegal or wrong about purchasing adult pornographic material made by and for consenting adults. However, organizations must be very careful when dealing with pornography in the workplace. As long as companies can show that they were taking reasonable steps to prevent pornography, they have a valid defense if they are subject to a sexual harassment lawsuit.
- Reasonable steps include establishing a computer usage policy that prohibits access to pornography sites, identifying those who violate the policy, and taking action against those users—regardless of how embarrassing it is for the users or how harmful it might be for the company.
- Sexting—sending sexual messages, nude or seminude photos, or sexually explicit videos over a cell phone—is a fast-growing trend that can lead to many problems for both senders and receivers.
- The Controlling the Assault of Non Solicited Pornography and Marketing (CAN-SPAM) Act specifies requirements that commercial emailers must follow when sending out messages that advertise a commercial product or service. The CAN-SPAM Act is also sometimes used in the fight against the dissemination of pornography.
- The proliferation of online sources of information and opinion means that the Internet is full of "news" accounts that are, in fact, highly opinionated, fictionalized, or satirical accounts of current events presented in journalistic style.

Key Terms

anonymous expression

anonymous remailer service

anti-SLAPP laws

Child Online Protection Act (COPA)

Children's Internet Protection Act (CIPA)

Communications Decency Act (CDA)

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM)

defamation

Digital Millennium Copyright Act (DMCA)

doxing

First Amendment

hate speech

Internet censorship

Internet filter

John Doe lawsuit

libel

Section 230 of the CDA

sexting

slander

strategic lawsuit against public participation (SLAPP)

Self-Assessment Questions

What is the basis for the protection of freedom of expression in the United States, and what types of expressions are not protected under the law?

1. The __________ protects Americans' rights to freedom of religion, freedom of expression, and freedom to peaceably assemble.
2. The Supreme Court has held that obscene speech and defamation may be forbidden by the government. True or False?
3. An important Supreme Court case that established a three-part test to determine if material is obscene and therefore not protected speech was __________.
4. Making either an oral or a written statement of alleged fact that is false and harms another person is __________.

What are some key federal laws that affect online freedom of expression, and how do they impact organizations?

5. Section 230 of the __________ provides immunity to an Internet service provider that publishes user-generated content, as long as its actions do not rise to the level of a content provider.
6. Which of the following laws required federally financed schools and libraries to use some form of technological protection to block computer access to obscene material, pornography, and anything else considered harmful to minors?
   a. Telecommunications Act
   b. Children's Internet Protection Act
   c. Child Online Protection Act
   d. Communications Decency Act

What important freedom of expression issues relate to the use of information technology?

7. The country with perhaps the most rigorous Internet censorship in the world is ______________.
   a. Brazil
   b. China
   c. Cuba
   d. United States
8. An anti-SLAPP law is used by government officials against citizens who oppose them on matters of public concern. True or False?
9. ______________ involves doing research on the Internet to obtain someone's private personal information (such as home address, email address, phone numbers, and place of employment) and even private electronic documents (such as photographs), and then posting that information online without permission.
10. An aggrieved party can file a ______________ lawsuit against a defendant whose identity is temporarily unknown because he or she is communicating anonymously or using a pseudonym.
11. The California State Court in *Pre-Paid v. Sturtz et al*. set a legal precedent that courts apply when deciding ______________.
    a. whether material is obscene
    b. if a library must install filters on its computers
    c. whether speech is merely annoying or hate speech
    d. whether or not to approve subpoenas requesting the identity of anonymous web posters
12. Persistent or malicious harassment aimed at an ethnic, racial, or religious group can be prosecuted as hate speech. True or False?
13. The ______________ Act specifies requirements that commercial emailers must follow when sending out messages that advertise or promote a commercial product or service.

Self-Assessment Answers

1. First Amendment; 2. True; 3. *Miller v. California*; 4. defamation; 5. Communications Decency Act; 6. b; 7. b; 8. False; 9. Doxing; 10. John Doe; 11. d; 12. False; 13. CAN-SPAM

Discussion Questions

1. Two frequently heard phrases associated with the topic of freedom of speech are: "I disapprove of what you say, but I will defend to the death your right to say it" and "It is easy to believe in freedom of speech for those with whom we agree." Craft a phrase that communicates your feelings about freedom of speech.
2. To what degree does monitoring of Internet activity by various government agencies impact your freedom of expression? Explain your answer.

3. What is a SLAPP? Under what conditions might a corporation employ a SLAPP? What are some actions that could be taken to counteract a SLAPP?
4. Have you ever posted or viewed copyrighted material online that could be subject to a DMCA takedown request? Research the case of *Lenz v. Universal Music Corp*. to learn the key issues it raised in connection with takedown orders. Write a few paragraphs summarizing your findings, including the current status of the case.

5. Outline a scenario in which you might be acting ethically but might still want to remain anonymous while using the Internet. Identify two approaches someone might take to learn your identity even if you attempt to remain anonymous.
6. What actions could an ISP take to censor the flow of information from you to others? What might motivate an ISP to take these actions?
7. How would you clearly distinguish between hate speech versus speech that is merely annoying, critical, or offensive? Would you be willing to defend someone's right to use annoying, critical, or offensive speech? How would you respond if such speech were directed at you?
8. Why must U.S. organizations be careful when dealing with issues relating to pornography in the workplace? What are some reasonable and legal steps an organization can take to limit pornography in the workplace?
9. Do research online to locate an anonymous remailer. Find out what is required to sign up for this service and what fees are involved. What guarantees of anonymity are made?
10. Look carefully at the email you receive over the next few days. Are any of the emails advertisements for a commercial product or service that violate the CAN-SPAM Act? If so, what can you do to stop receiving such emails in the future?
11. What is a John Doe lawsuit? Do you think that a corporation should be allowed to use a subpoena to identify a John Doe before proving that the person has done damage to the company? Why or why not? Under what conditions will the courts execute a John Doe lawsuit?
12. What are some of the key issues that must be considered when trying to determine if material on the Internet is obscene?
13. How did the CIPA escape from being ruled unconstitutional? Talk to your local librarian and find out if the library has implemented Internet filtering. If so, has it experienced any problems enforcing the use of filters? Write a short paragraph summarizing your findings.
14. Do research online to learn what personal information about you can be gleaned from various sources. Write a paragraph documenting your research and ultimate success or failure.
15. Think back over the last year or so and identify the "fake news" story that you feel caused the most controversy. What harm might have been caused by this story? Did you forward or relate this story in any way to your acquaintances, friends, or family?
16. Go online to find the code of ethics of the Society of Professional Journalists. Do you feel that this set of core principles should also apply to the nonprofessional online journalist? Why or why not?

17. Privacy, anonymity, and freedom of expression are all interrelated. However, with increased privacy and anonymity comes the capability for bad actors (e.g., criminals and terrorists) to conceal their communications and actions. Should governments and law enforcement agencies be given the ability to circumvent privacy and anonymity measures under certain circumstances? If so, what are those circumstances and how can freedom of expression abuse be avoided?

What Would You Do?

Use the five-step decision-making process discussed in Chapter 1 to analyze the following situations and recommend a course of action.

1. You run a small bakery and are shocked when friends tell you about several negative reviews of your bakery on Yelp. After reading the reviews, you have a very strong suspicion that they were all written by a neighbor with whom you have had several disagreements over the past year. The next day, you see this neighbor on the street in front of your house. What do you do?
2. A coworker confides to you that he is going to begin sending emails to your employer's internal corporate blog site, which serves as a suggestion box. He plans to use an anonymous remailer and sign the messages "Anonymous." Your friend is afraid of retribution from superiors but wants to call attention to instances of racial and gender discrimination observed during his five years as an employee with the firm. What would you say to your friend?
3. A college friend of yours approaches you about an idea to start an online reputation-management firm. One tactic the firm would use is to threaten those posting negative reviews and comments about your clients with a libel lawsuit unless they remove their posting. Should that fail, your firm would generate dozens of positive postings to outweigh the negative posting. What would you say to your friend about her idea?
4. Imagine that you receive a strongly worded hate email at your school or job that threatens physical violence toward you. What would you do? Does your school or workplace have a policy that covers such issues?
5. You are a member of your company's computer support group and have just helped someone from the company's board of directors upgrade his computer. As you run tests after making the upgrade, you are shocked to find dozens of child pornography videos on the hard drive. What would you do?
6. A friend contacts you about joining her company, Anonymous Remailers Anonymous. She would like you to lead the technical staff and offers you a 20 percent increase in salary and benefits over your current position. Your initial project would be to identify and implement changes necessary to provide increased protection for users of the company's anonymous remailer service. After discussing the opportunity with your friend, you suspect that some of the firm's customers are criminal types and purveyors of pornography and hate mail. Although your friend cannot be sure, she admits it is possible that hackers and terrorists may use her firm's services. Would you accept the generous job offer? Why or why not?

Cases

1. Techdirt Sued for Defamation

Techdirt was started in 1997 by Mike Masnick and grew into a blog that analyzes and offers insight into news stories about changes in government policy, technology, and legal issues that affect companies' ability to innovate and grow. The blog averages 1.5 million visitors per month, with over 65,000 posts and more than 1.4 million comments.

Dr. Shiva Ayyadurai has proclaimed himself to be the inventor of email and has filed a $15 million defamation lawsuit against the Techdirt website and its founder Mick Masnick for expressing doubts as to his claim. Ayyadurai is being represented by Charles Harder, a Beverly Hills attorney who became famous by filing multiple lawsuits against the Gawker blog site ("the source for daily Manhattan media news and gossip") that eventually forced that company into bankruptcy. Ayyadurai contends that a series of posts on Techdirt are libelous because the posts call Ayyadurai the "fake email inventor" and a "fraudster" and states his claims to have invented email are "bogus."

Ayyadurai maintains a website called The Inventor of Email and that describes his involvement with early email systems. According to the website, Ayyadurai had a goal of building a simple communication system that everyone could use to quickly and reliably send and receive digital messages. He designed his system based on a thorough analysis of the paper-based mail systems used in organizations around the world in the mid-1970s. He identified that the essential features of these systems included functions corresponding to "Inbox," "Outbox," "Drafts," "Memo", "To:", "From:", "Date:", "Subject:", "Body:", "Cc:", "Bcc:", "Attachments," "Folders," "Compose," "Forward," "Reply," "Address Book," "Groups," "Return Receipt," and "Sorting." He provided these capabilities in a software program with an interface so simple that users needed no expertise in computer systems to use it efficiently to "Send" and "Receive" mail electronically. He claims that it is these features that make his program "email" and that distinguish his program from prior electronic communications systems.

Harder, on behalf of Ayyadurai, sent a letter to Diaspora, a social networking platform, demanding that certain posts supportive of Techdirt be removed. The letter claims that these posts are defamatory, violate Diaspora's terms of service, and "constitute harassment and intentional infliction of emotional distress."

On the other hand, historians point out that email began long before 1978. For example, there was a messaging system called MAILBOX at MIT in 1965. Ray Tomlinson is frequently credited with inventing the modern concept of email for the Internet in 1972. By 1975, there were things such as email folders (invented by Larry Roberts) and some other basic email apps. These early email programs were basic and elementary but by 1978 they had essentially all the features that Ayyadurai claims to have invented.

Ed Klaris, a long-time media lawyer in New York, says "This is a classic scientific debate, which is a cornerstone of the First Amendment, second only to political debate. Theories of who invented something as basic as email software code need to be free and open and not constrained by claims of libel."

Mounting a defense against this lawsuit may prove very costly and time-consuming for Masnick and his small company. Says Masnick: "In our view, this is not a fight about who invented email. This is a fight about whether or not our legal system will silence independent publications for publishing opinions that public figures do not like. And here's the thing: this fight could very well be the end of Techdirt, even if we are completely on the right side of the law."

Critical Thinking Questions

1. Visit the Techdirt blog site at https://www.techdirt.com/ and read several of its postings over a period of a few weeks. Do you think that Techdirt is an important independent media resource worth protecting or should it be subject to strong scrutiny and pressure to shut down? Explain your answer.
2. Visit the Inventor of Email's website at http://www.inventorofemail.com/. View the video there and read several of the postings found there. Do you think that Ayyadurai presents a strong and convincing argument that he invented email? Why or why not?
3. What measures might Masnick take to defend himself and his organization in this defamation lawsuit? What measures might Ayyadurai and his attorney take to strengthen his case against Masnick? Is demanding that social media sites take down posts supporting Masnick a winning strategy? Why or why not?

Sources: "About Techdirt," https://www.techdirt.com/about.php (accessed January 27, 2017); Jeff John Roberts, "'Inventor of Email' Slaps Tech Site with $15M Libel Suit for Mocking His Claim," *Fortune*, January 5, 2017, http://fortune.com/2017/01/05/email-inventor-techdirt/; David Kravets, "Man Who Says He Invented Email Sues Techdirt for Disputing His Claim," *ars Technica*, January 6, 2017, https://arstechnica.com/tech-policy/2017/01/man-who-says-he-invented-e-mail-sues-techdirt-for-disputing-claim/; "The Inventor of Email," http://www.inventorofemail.com/ (accessed January 27, 2017); "Legal Threats by Charles Harder & Shiva Ayyadurai Targeting More Speech," *Techdirt*, https://www.techdirt.com/blog/?tag=defamation; John Biggs, "Media Blog Techdirt Fights for Its Life in Frivolous Lawsuit," *Techdirt*, January 12, 2017, https://techcrunch.com/2017/01/12/media-blog-techdirt-fights-for-its-life-in-frivolous-lawsuit/.

2. China's Great Firewall

China has a population of over 1.4 billion people, and more than 700 million of its citizens are Internet users. Given those statistics, it is perhaps not surprising that China is the world's leader in e-commerce, with 40 percent of global sales volume—double that of the United States. China is also the home of 4 of the world's top 12 Internet companies ranked by market capitalization: e-commerce giant Alibaba, social-media and gaming company Tencent, search specialist Baidu, and smartphone maker Xiaomi. China has accomplished all this while implementing a system of Internet censorship and surveillance measures, dubbed the Golden Shield Project and the Great Firewall, which are some of the strictest in the world.

China's attempt to control access and limit content available to its citizens began shortly after the Internet's introduction in China. The country's Golden Shield Project and the Great Firewall are part of an immense, multifaceted Internet surveillance and content control system that is augmented by workers who delete and add posts to spin any debate in favor of the government's stance. The goal of the Chinese government is to block all content it deems undesirable, particularly news stories that are unfavorable to China or its leaders, as well as references to infamous events, such as the 1989 Tiananmen Square Massacre. While the Golden Shield Project is focused on domestic sites, the Great Firewall stands at the international gateways, keeping out unwanted foreign sites using a sophisticated and multitiered system. According to Simon Denyer, the *Washington Post*'s bureau chief in China, "The Great Firewall is an attempt to bridge one of the country's most fundamental contradictions—to have an economy intricately connected to the outside world but a political culture closed off from such 'Western values' as free speech and democracy."

Chinese Internet users have their own censored versions of popular services, including Baidu (instead of Google), Weibo (instead of Twitter), WeChat (instead of Facebook), and Youku (instead of YouTube). In addition, the Great Firewall blocks roughly 25 percent of all Internet sites, including the Chinese and English news websites of the Reuters news agency, Bloomberg LP, the *Guardian*, and the *New York Times* so that they are inaccessible in China.

Some Chinese Internet users are able to gain access to restricted content through the use of virtual private networks (VPNs), which help users elude the restrictions of the Great Firewall by changing the IP address on their computer, laptop, or mobile device into one of many offered by the VPN provider. So, while a user may be accessing the Internet from a city within China, the VPN makes it look like the user is in Japan or some other country where Internet access is unrestricted. In addition, once users activate their VPN, they are connected to one of its servers via a dedicated, encrypted link, ensuring all of the data flowing back and forth between their device and the VPN server are private. However, VPNs exist at the pleasure of the Chinese Communist Party and can be shut down at any time. Indeed, the government recently began blocking VPNs on which thousands relied to circumvent the Great Firewall. Even with the option of using VPN, many Chinese are content to stay within the state-controlled version of the Internet. A recent study indicated that less than 3 percent of Chinese try to jump the Great Firewall to browse the open Internet.

According to the nationalist state-owned *Global Times* newspaper, “It requires a sophisticated capability to keep out harmful ideas without damaging the nation’s global connectivity. It enables China to communicate with the outside world, meanwhile Western opinion cannot easily penetrate as ideological tools.”

Critical Thinking Questions

1. It is estimated that by 2024, roughly five billion people will be connected to the Internet, with the biggest increases in societies that are severely censored. Many observers are concerned that the Chinese Internet-sovereignty model—where the government controls the flow of information and access to the Internet within its borders—will become much more prevalent in many of these countries. Can you describe an alternative Internet-sovereignty model that might be acceptable for these countries yet still allow some modicum of freedom of expression?
2. Some freedom of expression advocates are concerned that U.S.-based technology firms will do whatever it takes to gain a foothold in the Chinese market, even going so far as to implement surveillance and censorship measures in their products and services in order to meet the demands of the Chinese government. How might global Internet users react to a Facebook or YouTube that censors its users’ posts and monitors its users to comply with laws in China? What ethical and economic factors should an information technology company weigh when considering whether to enter the Chinese marketplace?
3. Can you identify any barriers to freedom of expression on the Internet that not only are acceptable to you but you would like to see implemented?

Sources: James Griffiths, “Great Firewall Rising: How China Wages Its War on the Internet,” *CNN*, October 25, 2015, www.cnn.com/2015/10/25/asia/china-war-internet-great-firewall/; Kristie Lu Stout, “China’s Great Firewall: Fortune at the Expense of Freedom?” *CNN*, March 25, 2015, www.cnn.com/2015/03/25/asia/china-internet-censorship-kristie-lu-stout; Orlando Crowcroft, “Behind the Great Firewall, China Is Winning Its War against Internet Freedom,” *IB Times*, May 9, 2016, www.ibtimes.co.uk/behind-great-firewall-china-winning-its-war-against-internet-freedom-1558550; Simon Denyer, “China’s Scary Lesson to the World: Censoring the Internet Works,” *Washington Post*, May 23, 2016, https://www.washingtonpost.com/world/asia_pacific

/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html; Tripp Mickle and Lukas I. Alpert, “Apple Pulls New York Times App from China Store,” *Wall Street Journal*, January 4, 2017, www.wsj.com/articles/apple-pulls-new-york-times-app-from-china-store-1483576379; “China and the Internet: A Force, but Not for Democracy,” *The Economist*, www.economist.com/blogs/analects/2013/04/china-and-internet.

End Notes

[1] “About Tor,” Tor, https://www.torproject.org/about/overview (accessed January 11, 2017).

[2] Cara McGoogan, “Dark Web Browser Tor Is Overwhelmingly Used for Crime, Says Study,” *The Telegraph*, February 2, 2016, http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/.

[3] Quentin Hardy, “Daily Report: Gawker and Truth,” *New York Times*, August 25, 2016, www.nytimes.com/2016/08/26/technology/daily-report-gawker-and-truth.html?rref=collection%2Ftimestopic%2FGawker%20Media&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=4&pgtype=collection&_r=0.

[4] Courtney Macavinta, “The Supreme Court Today Rejected the Communications Decency Act,” *CNET,* June 26, 1997, http://news.cnet.com/High-court-rejects-CDA/2009-1023_3-200957.html.

[5] *Reno, Attorney General of the United States v. American Civil Liberties Union, et al.*, 521 U.S. 844 (1997), Legal Information Institute, Cornell University Law School, www.law.cor-nell.edu/supct/html/96-511.ZS.html (accessed January 26, 2013).

[6] “Section 230 of Communications Decency Act Does Not Provide an Absolute Immunity,” Traverse Legal, July 2, 2009, http://section230communicationsdecencyact1996.com.

[7] Josh Constine, “How Facebook News Feed Works,” *Tech Crunch*, September 6, 2016, https://techcrunch.com/2016/09/06/ultimate-guide-to-the-news-feed/.

[8] Title XIV—Child Online Protection Act, Electronic Privacy Information Center, http://epic.org/free_speech/censorship/copa.html (accessed January 26, 2013).

[9] *Ashcroft v. American Civil Liberties Union* (03-218), 542 U.S. 656 (2004), Legal Information Institute, Cornell University Law School, www.law.cornell.edu/supct/html/03-218.ZS.html (accessed January 26, 2013).

[10] Renee Shipley, “The Best Internet Filter Software of 2016,” *Top Ten Reviews*, July 16, 2016, www.toptenreviews.com/software/security/best-internet-filter-software/.

[11] “About ClearSail/Family.NET,” ClearSail/Family.NET, www.clearsail.net/about.htm (accessed January 20, 2017).

[12] Federal Communications Commission, “Children’s Internet Protection Act: FCC Consumer Facts,” www.fcc.gov/cgb/consumerfacts/cipa.html (accessed January 26, 2013).

[13] Emma Lansso, “Court Flouts First Amendment, OKs Libraries’ Internet Censorship Scheme,” Center for Democracy & Technology, April 13, 2012, https://cdt.org/blog/court-flouts-first-amendment-oks-libraries-internet-censorship-scheme/.

[14] John Gantz and Jack B. Rochester, *Pirates of the Digital Millennium* (Harlow, UK: Financial Times Prentice Hall, 2005).

[15] Ian C. Schick and Edward A. Cavazos, “The Case of Prince, a Dancing Baby and the DMCA Takedown Notice,” The Internet and Social Media Law Blog (posted September 28, 2015), www.socialgameslaw.com/2015/09/the-case-of-prince-a-dancing-baby-and-the-dmca-takedown-notice.html.

[16] Jonathan Zittrain and Benjamin Edelman, “Empirical Analysis of Internet Filtering in China,” Berkman Center for Internet & Society, Harvard Law School, http://cyber.law.harvard.edu/filtering/china/ (accessed January 26, 2013).

[17] Danny O’Brien, “Is Brazil the Censorship Capital of the Internet? Not Yet,” *CPJ Blog,* Committee to Protect Journalists, April 28, 2010, www.cpj.org/blog/2010/04/is-brazil-the-censorship-capital-of-the-internet.php.

[18] Josefina Salomon, “Six Facts about Censorship in Cuba,” Amnesty International, March 11, 2016, https://www.amnesty.org/en/latest/campaigns/2016/03/six-facts-about-censorship-in-cuba.

[19] Rose Eveleth, “The United States Is Declared an Enemy of the Internet by Reporters without Borders,” *Smithsonian Magazine*, March 19, 2014, www.smithsonianmag.com/smart-news/united-states-declared-enemy-internet-reporters-without-borders-180950169/#C2izZpPdo5RpcvEk.99.

[20] Josh Harkinson, “Yelp Is Pushing a Law to Shield Its Reviewers from Defamation Suits,” *Mother Jones*, July 20, 2015, www.motherjones.com/politics/2015/07/yelp-slapp-lawsuit-legislation-speak-free-act.

[21] First Amendment Project, “Guarding Against the Chill: A Survival Guide for SLAPP Victims,” https://www.thefirstamendment.org/media/Guarding-Against-the-Chill.pdf (accessed January 27, 2013).

[22] First Amendment Project, “Guarding Against the Chill: A Survival Guide for SLAPP Victims,” https://www.thefirstamendment.org/media/Guarding-Against-the-Chill.pdf (accessed January 27, 2013).

[23] Josh Harkinson, “Yelp Is Pushing a Law to Shield Its Reviewers from Defamation Suits,” *Mother Jones*, July 20, 2015, www.motherjones.com/politics/2015/07/yelp-slapp-lawsuit-legislation-speak-free-act.

[24] “U.S. Needs an Anti-SLAPP Law Like California’s,” *Los Angeles Times*, August 16, 2015, www.latimes.com/opinion/editorials/la-ed-slapp-20150816-story.html.

[25] Frank Rich, “Journal; The 2 Tim McVeighs,” *New York Times*, January 17, 1998, www.nytimes.com/1998/01/17/opinion/journal-the-2-tim-mcveighs.html?n=Top/Reference/Times%20Topics/Subjects/H/Homosexuality.

[26] “Doxing and Cyberbullying,” Cyberbullying Research Center, September 16, 2015, http://cyberbullying.org/doxing-and-cyberbullying.

[27] Ms. Smith, “Judge Cites Use of Secure Email Riseup as a Potential Terrorist Indicator,” *Network World*, January 11, 2015, www.networkworld.com/article/2867329/microsoft-subnet/judge-cites-use-of-secure-email-riseup-as-a-potential-terrorist-indicator.html.

[28] “*Pre-Paid Legal v. Sturtz Case Archive*,” Electronic Frontier Foundation. http://w2.eff.org/Censorship/SLAPP/Discovery_abuse/PrePaid_Legal_v_Sturtz/?f=20010712_proposed_or-der.html (accessed January 26, 2013).

[29] *John Doe v. 2TheMart.com Inc.*, Berkman Center for Internet & Society, Harvard Law School, http://cyber.law.harvard.edu/stjohns/2themart.html (accessed January 30, 2013).

[30] YouTube, "Terms of Service," www.youtube.com/t/terms (accessed March 11, 2013).

[31] YouTube, "YouTube Community Guidelines," www.youtube.com/t/community_guidelines (accessed March 11, 2013).

[32] Leila Cobo, "Gerardo Ortiz Apologizes for Graphic 'Fuiste Mia' Video, but Should He Be Prosecuted?," *Billboard*, July 22, 2016, http://www.billboard.com/articles/columns/latin/7446673/gerardo-ortiz-apologizes-fuiste-mia-video-arrest.

[33] Griselda Flores, "Gerardo Ortiz's Controversial 'Fuiste Mia' Music Video Removed from YouTube" *Billboard*, April 11, 2016, www.billboard.com/articles/columns/latin/7326585/gerardo-ortiz-fuiste-mia-music-video-removed-youtube.

[34] "The Stats on Internet Pornography," *Information2Share*, December 12, 2012, http://information2share.wordpress.com/2012/12/12/the-stats-on-internet-pornography/.

[35] Gilbert Wondracek, Thorsten Holz, Christian Platzer, Engin Kirda, and Christopher Kruegel, "Is the Internet for Porn? An Insight into the Online Adult Industry," International Secure Systems Lab, www.iseclab.org/papers/weis2010.pdf (accessed January 31, 2013).

[36] Jerry Ropelato, "Internet Pornography Statistics," *TopTenReviews,* http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html#anchor2 (accessed January 31, 2013).

[37] *Ashcroft v. American Civil Liberties Union* (03-218), 542 U.S. 656 (2004), Legal Information Institute, Cornell University Law School, www.law.cornell.edu/supct/html/03-218.ZS.html (accessed January 30, 2013).

[38] Eric Goldman, "Internet Obscenity Conviction Requires Assessment of National Community Standards—*United States v. Kilbride*" *Technology & Marketing Law Blog*, October 30, 2009, blog.ericgoldman.org/archives/2009/10/internet_obscen.htm.

[39] Cheryl Conner, "Who Wastes the Most Time at Work?" *Forbes*, September 7, 2013, www.forbes.com/sites/cherylsnappconner/2013/09/07/who-wastes-the-most-time-at-work/#3b46a78b7b3a.

[40] Randye Hoder, "Study Finds Most Teens Sext before They're 18," *Time*, July 3, 2014, http://time.com/2948467/chances-are-your-teen-is-sexting/.

[41] Emil Protalinski, "Facebook Spammer Fined $1 Billion for Over 4 Million Posts," *TechSpot*, October 6, 2010, www.techspot.com/news/40553-facebook-spammer-fined-1-billion-for-over-4-million-posts.html.

[42] Ken Magill, "Porn CAN-SPAM Conviction Upheld," *Direct*, September 11, 2007, http://directmag.com/email/news/porn_can-spam_conviction/#.

[43] " 'Spam King' Sentenced to Two Years in Prison," BBC, June 15, 2016, http://www.bbc.com/news/technology-36538541.

[44] Monica Anderson and Andrea Caumont, "How Social Media Is Reshaping News," Pew Research Center, September 24, 2014, http://www.pewresearch.org/fact-tank/2014/09/24/how-social-media-is-reshaping-news/.

CHAPTER **6**

INTELLECTUAL PROPERTY

QUOTE

Notwithstanding the fact that the most innovative and progressive space we've seen—the Internet—has been the place where intellectual property has been least respected. You know, facts don't get in the way of this ideology.

—Lawrence Lessig, the Roy L. Furman Professor of Law and Leadership at Harvard Law School, political activist and author

arka38/Shutterstock.com

ORGANIZATIONS BEHAVING BADLY

For years, Apple and Samsung have traded accusations about the unlawful copying of various features used in each company's smartphones and tablets. Those accusations ultimately led to multiple competing lawsuits, with each company alleging patent infringement by the other. The fallout began in 2010, when Apple first warned Samsung that the South Korean manufacturer's tablets and smartphones infringed on Apple patents. Apple, however, did not immediately sue Samsung because the manufacturer was also a key supplier, from whom Apple purchased billions of dollars' worth of screens, processors, and other components. Instead, executives from the two companies met to settle their issues but were ultimately unable to agree on a resolution.

After negotiations broke down, Apple sued Samsung in April 2011 for alleged infringement of various Apple design patents. These patents covered the black rectangle shape and rounded corners, the bezel, and the graphical layout of icons on the iPhone. Samsung countersued for infringement on some of its own patents and also filed claims against Apple in Germany, Japan, and South Korea. Apple won the first round of the battle and was awarded $1 billion in damages. Additional trials ensued over the amount of damages, with the net result that Samsung still owed over $900 million. In December 2015, Samsung agreed to pay Apple $548 million to settle the original patent infringement lawsuit.[1]

In another suit filed against Samsung in February 2012, Apple accused Samsung of infringing additional different patents on newer Samsung smartphones, claiming damages of $2.2 billion. Again, Samsung countersued, claiming that Apple was trying to hurt competition by targeting it for litigation and alleging Apple had infringed some of its patents in connection with camera and folder functionality and video transmission technology used in Apple's FaceTime app. This time the jury ordered Samsung to pay $119.6 million for infringement, much less than the $2.2 billion the iPhone maker had sought. Concurrently, Apple was ordered to pay Samsung $158,400 for infringing one of the Korean company's two patents.

Although these lawsuits involve Apple and Samsung, the larger battle actually pits Apple against Google, which developed the Android operating system—which runs on many of Samsung's smartphones and which Apple alleges was illegally based on its iPhone and iOS operating system. In

2010, Steve Jobs told his biographer: “I will spend my last dying breath if I need to, and I will spend every penny of Apple’s $40 billion in the bank, to right this wrong. I’m going to destroy Android because it is a stolen product.”[2]

Rather than suing Google—which technically does not generate revenue directly from Android because it provides it to hardware makers at no cost—Apple has followed a strategy of suing companies that use the Android operating system, including Motorola Mobility, HTC, Nokia, and Nikon. Many industry observers have noted that the lawsuits seem to be part of a broader Apple strategy to cut into the sales of devices using Android, which has become the dominant mobile operating system worldwide. Apple doesn’t just want to inflict monetary damages; it wants Android phones barred from sale. The most effective way to do this is to sue the device makers, who already earn a relatively low profit margin per device. If the device makers must pay damages to Apple, they will be unable to earn a good return on their phones, potentially forcing them out of the phone business.[3] After the verdict in the 2012 lawsuit was announced, however, some members of the jury suggested that Apple and Google confront each other directly, rather than dragging handset makers such as Samsung into court.

In the meantime, Apple and Samsung appealed the case to their U.S. Supreme Court—the first time a design patent case has been examined by the Supreme Court since the 1800s.[4] In December 2016, the Supreme Court ruled in favor of Samsung and unanimously reversed an earlier appeals court ruling that the company must pay $399 million to Apple. The Court’s reasoning was that it’s possible for a design patent to only cover part of a product rather than all of it. So just because a company’s product copies one or two features from a competitor it doesn’t necessarily mean it has to forfeit all of that product’s profits to its competitor. The case now goes back to a lower court to reevaluate how much Samsung must pay in damages for copying iPhone features.

What design features of a product that determine the "look and feel" of a product can be patented, and how are reasonable damages determined if such a patent is infringed? Is the current system of protecting intellectual property through patents, copyrights, trademarks, and trade secrets encouraging innovation or stifling it?[5]

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What does the term *intellectual property* encompass, and what measures can organizations take to protect their intellectual property?
2. What are some of the current issues associated with the protection of intellectual property?

WHAT IS INTELLECTUAL PROPERTY?

Intellectual property is a term used to describe works of the mind—such as art, books, films, formulas, inventions, music, and processes—that are distinct and owned or created by a single person or group. It is protected through copyright, patent, and trade secret laws.

Copyright law protects authored works, such as art, books, film, and music; patent law protects inventions; and trade secret law helps safeguard information that is critical to an organization's success. Together, copyright, patent, and trade secret laws form a complex body of law that addresses the ownership of intellectual property. Such laws can also present potential ethical problems for IT companies and users—for example, some innovators believe that copyrights, patents, and trade secrets stifle creativity by making it harder to build on the ideas of others. Meanwhile, the owners of intellectual property want to control and receive compensation for the use of their intellectual property. Should the need for ongoing innovation or the rights of property owners govern how intellectual property is used?

Defining and controlling the appropriate level of access to intellectual property are complex tasks. For example, protecting computer software has proven to be difficult because it has not been well categorized under the law. Software has sometimes been treated as the expression of an idea, which can be protected under copyright law. In other cases, software has been treated as a process for changing a computer's internal structure, making it eligible for protection under patent law. At one time, software was even judged to be a series of mental steps, making it inappropriate for ownership and ineligible for any form of protection.

Copyrights

Copyright and patent protection was established through the U.S. Constitution, Article I, section 8, clause 8, which specifies that Congress shall have the power "to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Rights to their respective Writings and Discoveries."

A **copyright** is the exclusive right to distribute, display, perform, or reproduce an original work in copies or to prepare derivative works based on the work. Copyright protection is granted to the creators of "original works of authorship in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device."[6] The author may grant this exclusive right to others. As new forms of expression develop, they can be awarded copyright protection. For example, in the Copyright Act of 1976, audiovisual works were given protection, and computer programs were assigned to the literary works category.

Copyright infringement is a violation of the rights secured by the owner of a copyright. Infringement occurs when someone copies a substantial and material part of another's copyrighted work without permission. The courts have a wide range of discretion in awarding damages—from $200 for innocent infringement to $100,000 for willful infringement.

Copyright Term

Copyright law guarantees developers the rights to their works for a certain amount of time. Since 1960, the term of copyright has been extended 11 times from its original limit of 28 years. The Copyright Term Extension Act, also known as the Sonny Bono Copyright Term Extension Act (after the legislator, and former singer/entertainer, who was one of the cosponsors of the bill in the House of Representatives), signed into law in 1998, and established the following time limits:

- For works created after January 1, 1978, copyright protection endures for the life of the author plus 70 years.
- For works created but not published or registered before January 1, 1978, the term endures for the life of the author plus 70 years, but in no case expires earlier than December 31, 2004.
- For works created before 1978 that are still in their original or renewable term of copyright, the total term was extended to 95 years from the date the copyright was originally secured.[7]

These extensions were primarily championed by movie studios concerned about retaining rights to their early films. Opponents argued that extending the copyright period made it more difficult for artists to build on the work of others, thus stifling creativity and innovation. The Sonny Bono Copyright Term Extension Act was legally challenged by Eric Eldred, a bibliophile who wanted to put digitized editions of old books online. The *Eldred v. Ashcroft* case went all the way to the Supreme Court, which ruled the act constitutional in 2003.[8]

Eligible Works

The types of work that can be copyrighted include architecture, art, audiovisual works, choreography, drama, graphics, literature, motion pictures, music, pantomimes, pictures, sculptures, sound recordings, and other intellectual works, as described in Title 17 of the U.S. Code. To be eligible for a copyright, a work must fall within one of the preceding categories, and it must be original. Copyright law has proven to be extremely flexible in covering new technologies; thus, software, video games, multimedia works, and web pages can all be protected. However, evaluating the originality of a work is not always a straightforward process, and disagreements over whether or not a work is original sometimes lead to litigation.

Copyright infringement lawsuits are common in the world of music, with many of the major artists having gone through such a lawsuit at some point in their careers. For example, former Beatles member George Harrison was entangled for decades in litigation over similarities between his hit "My Sweet Lord," released in 1970, and "He's So Fine," composed by Ronnie Mack and recorded by the Chiffons in 1962.[9] Harrison was found guilty of "subconscious plagiarism" and had to pay $1.6 million of the earnings from "My Sweet Lord" to Bright Tunes (songwriter Ronnie Mack had died in 1963).[10]

Some works are not eligible for copyright protection, including those that have not been fixed in a tangible form of expression (such as an improvisational speech) and those that consist entirely of common information that contains no original authorship, such as a chart showing conversions between European and American units of measure.

Fair Use Doctrine

Copyright law tries to strike a balance between protecting an author's rights and enabling public access to copyrighted works. The **fair use doctrine** was developed over the years as courts worked to maintain that balance. It allows portions of copyrighted materials to be used without permission under certain circumstances. Title 17, Section 107, of the U.S. Code established that courts should consider the following four factors when deciding whether a particular use of copyrighted property is fair and can be allowed without penalty:

1. The purpose and character of the use (such as commercial use or nonprofit, educational purposes)
2. The nature of the copyrighted work
3. The portion of the copyrighted work used in relation to the work as a whole
4. The effect of the use on the value of the copyrighted work[11]

The concept that an idea cannot be copyrighted but the expression of an idea can be key to understanding copyright protection. For example, an author cannot copy the exact words that someone else used to describe his feelings during a skirmish with terrorists, but he can convey the sense of horror that the other person expressed. Also, there is no copyright infringement if two parties independently develop a similar or even identical work. For example, if two writers happened to use the same phrase to describe a key historical figure, neither would be guilty of infringement. Of course, independent creation can be extremely difficult to prove or disprove.

Since 2004, Google has scanned and converted into machine readable form over 20 million books as part of a project to create an electronic searchable database of books. Users of the Google Books service can enter search queries and view full pages from books in which the search terms appear, provided that either the book is out of copyright or the copyright owner has given permission for the work to be included in the database. If the book is still under copyright, a user sees "snippets" of text around the queried search terms. The Authors Guild, a professional organization that advocates for authors on issues of copyright, fair contracts, and free speech, sued Google saying that serving up search results from scanned books infringes on publishers' copyrights. In April 2016, the Supreme Court let stand a lower court decision that rejected the writers' claims on the basis that such usage represented noninfringing fair use. The ruling allows Google to continue with its scanning project and may encourage other digitization projects.[12]

Software Copyright Protection

The use of copyrights to protect computer software raises many complicated issues of interpretation. For example, a software manufacturer can observe the operation of a competitor's copyrighted program and then create a program that accomplishes the same result and performs in the same manner. To prove infringement, the copyright holder must show a striking resemblance between its software and the new software that could be explained only by copying. However, if the new software's manufacturer can establish that it developed the program on its own, without any knowledge of the existing program, there is no infringement. For example, two software manufacturers could conceivably develop separate but nearly identical programs for a simple game such as tic-tac-toe without infringing the other's copyright.

Registering a copyright for a software program is a simple process. The individual or organization that owns the software must complete a brief application form that requests basic information such as the title of the program, who created the program and when, and who owns the copyright. The copyright holder then just needs to send the application, along with a small fee and a copy of the program, to the U.S. Copyright Office.[13]

Java is a widely used programming language developed at Sun Microsystems during the early 1990s. Today it is the most popular programming language for developing Android smartphone applications and is also used to code the software that runs many routers, switches, and other network devices. Google wrote its own version of Java to implement the Android OS used in smartphones, but in order to allow developers to write their own programs for Android, Google's implementation used the same names, organization, and functionality as the Java application program interfaces (APIs).[14] (An API is a set of codes and protocols that enable programs to interact with one another. For example, when you read an article online and click on an icon to share that article via Facebook, you are using a Facebook API that the website hosting that article got from Facebook.)

Google and Sun originally discussed a potential partnership that would include licensing deals for Java, but were unable to reach an agreement. Software giant Oracle purchased Sun in 2010 and continued to discuss a licensing deal with Google, but, again, could not reach an agreement. Oracle then sued Google for copyright and patent infringement. In the initial hearing of the case, the jury found there was no infringement whatsoever. Oracle appealed to the Federal Circuit Court of Appeals, which reversed the district court, sending the case back to the district court for reconsideration—with Oracle seeking damages of up to $9 billion. In May 2016, the jury found that Android did not infringe Oracle-owned copyrights because Android's reimplementation of 37 Java APIs represented fair use.[15] Oracle appealed this decision in October 2016.

This case is of interest to many in the software development industry. If owners of APIs are able to use copyright law to control how programming is done, it would result in a major change in software development practices. According to Mitch Stoltz, an attorney for the Electronic Frontier Foundation, such a ruling would "create a radical shift in how software is developed worldwide. If it requires permission each time APIs are used and code calls other code, then you've upended the economics of software."[16]

The Prioritizing Resources and Organization for Intellectual Property Act of 2008

The **Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008** (Public Law 110-403) created the position of Intellectual Property Enforcement Coordinator within the Executive Office of the President. It also increased trademark and copyright enforcement and substantially increased penalties for infringement. One of its programs, called Computer Hacking and Intellectual Property (CHIP), is a network of over 150 experienced and specially trained federal prosecutors who focus on computer and intellectual property crimes.[17]

The Organisation for Economic Cooperation and Development (an international organization comprised of the United States and 33 other countries) estimates that international trade in counterfeit and pirated goods could have accounted for as much as $461 billion or 2.5 percent of world trade in 2013.[18]

General Agreement on Tariffs and Trade

The General Agreement on Tariffs and Trade (GATT) was a multilateral agreement governing international trade. There were several rounds of negotiations addressing various trade issues. The Uruguay Round, completed in December 1993, resulted in a trade agreement among 117 countries. This agreement also created the World Trade Organization (WTO) in Geneva, Switzerland, to enforce compliance with the agreement. GATT includes a section covering copyrights called the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), discussed in the following section. The U.S. intellectual property law was amended to be essentially consistent with GATT through both the Uruguay Round Agreements Act of 1994 and the Sonny Bono Copyright Term Extension Act of 1998. Despite GATT, however, copyright protection varies greatly from country to country, and an expert should be consulted when considering international usage of any intellectual property.

The WTO and the WTO TRIPS Agreement (1994)

The WTO is a global organization that deals with the rules of international trade based on WTO agreements that are negotiated and signed by representatives of the world's trading nations. It is headquartered in Geneva, Switzerland, and has 164 member nations as of July 2016. The goal of the WTO is to help producers of goods and services, exporters, and importers conduct their business globally.[19]

Many nations recognize that intellectual property has become increasingly important in world trade, yet the extent of protection and enforcement of intellectual property rights varies around the world. As a result, the WTO developed the **Agreement on Trade-Related Aspects of Intellectual Property Rights**, also known as the TRIPS Agreement, to establish minimum levels of protection that each government must provide to the intellectual property of all WTO members. This binding agreement requires member governments to ensure that intellectual property rights can be enforced under their laws and that penalties for infringement are tough enough to deter further violations. Table 6-1 provides a brief summary of copyright, patent, and trade secret protection under the TRIPS Agreement.

TABLE 6-1 Summary of the WTO TRIPS agreement

Form of intellectual property	Key terms of agreement
Copyright	Computer programs are protected as literary works. Authors of computer programs and producers of sound recordings have the right to prohibit the commercial rental of their works to the public.
Patent	Patent protection is available for any invention—whether a product or process—in all fields of technology without discrimination, subject to the normal tests of novelty, inventiveness, and industrial applicability. It is also required that patents be available and patent rights enjoyable without discrimination as to the place of invention and whether products are imported or locally produced.
Trade secret	Trade secrets and other types of undisclosed information that have commercial value must be protected against breach of confidence and other acts that are contrary to honest commercial practices. However, reasonable steps must have been taken to keep the information secret.

Source: "Overview: The TRIPS Agreement," World Trade Organization, www.wto.org/english/tratop_e/trips_e/intel2_e.htm.

Many developing countries have taken the position that the TRIPS Agreement favors developed countries and transnational corporations at their expense. These countries argue that TRIPS imposes higher costs on developing countries in the form of more expensive drugs, agricultural products, and foreign-owned technologies.[20]

The World Intellectual Property Organization Copyright Treaty (1996)

The World Intellectual Property Organization (WIPO), headquartered in Geneva, Switzerland, is an agency of the United Nations established in 1967. WIPO is dedicated to "the use of intellectual property as a means to stimulate innovation and creativity." It has 185 member nations and administers 25 international treaties. Since the 1990s, WIPO has strongly advocated for the interests of intellectual property owners. Its goal is to ensure that intellectual property laws are uniformly administered.[21]

The WIPO Copyright Treaty, adopted in 1996, provides additional copyright protections to address electronic media. The treaty ensures that computer programs are protected as literary works and that the arrangement and selection of material in databases is also protected. It provides authors with control over the rental and distribution of their work and prohibits circumvention of any technical measures put in place to protect the works. The WIPO Copyright Treaty is implemented in the U.S. law through the Digital Millennium Copyright Act (DMCA), which is discussed in the next section.

The Digital Millennium Copyright Act (1998)

The DMCA (Public Law 105-304) was signed into law in 1998 and implements two 1996 WIPO treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. The act is divided into the following five sections:

1. *Title I (WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998)*—This section implements the WIPO treaties by making certain technical amendments to the U.S. law in order to provide

appropriate references and links to the treaties. It also creates two new prohibitions in the Copyright Act (Title 17 of the U.S. Code)—one on circumvention of technological measures used by copyright owners to protect their works and one on tampering with copyright management information. Title I also adds civil remedies and criminal penalties for violating the prohibitions.

2. *Title II (Online Copyright Infringement Liability Limitation Act)*—This section enables website operators that allow users to post content on their website (e.g., music, video, and pictures) to avoid copyright infringement liability if certain "safe harbor" provisions are followed.
3. *Title III (Computer Maintenance Competition Assurance Act)*—This section permits the owner or lessee of a computer to make or authorize the making of a copy of a computer program in the course of maintaining or repairing that computer. The new copy cannot be used in any other manner and must be destroyed immediately after the maintenance or repair is completed.
4. *Title IV (Miscellaneous provisions)*—This section adds language to the Copyright Act confirming the Copyright Office's authority to continue to perform the policy and international functions that it has carried out for decades under its existing general authority.
5. *Title V (Vessel Hull Design Protection Act)*—This section creates a new form of protection for the original design of vessel hulls.

The portion of Title I dealing with anticircumvention provisions makes it an offense to do any of the following:

- Circumvent a technical protection
- Develop and provide tools that allow others to access a technologically protected work
- Manufacture, import, provide, or traffic in tools that enable others to circumvent protection and copy a protected work

Violations of these provisions carry both civil and criminal penalties, including up to five years in prison, a fine of up to $500,000 for each offense, or both. Unlike traditional copyright law, the DMCA does not govern copying; instead, it focuses on the distribution of tools and software that can be used for copyright infringement as well as for legitimate noninfringing use. Although the DMCA explicitly outlaws technologies that can defeat copyright protection devices, it does permit reverse engineering for encryption, interoperability, and computer security research.

Several cases brought under the DMCA have dealt with the use of software to enable the copying of DVD movies. For example, motion picture companies supported the development and worldwide licensing of the Content Scramble System (CSS), which enables a DVD player or a computer drive to decrypt, unscramble, and play back motion pictures on DVDs, but not copy them. However, a software program called DeCSS can break the encryption code and enable users to copy DVDs. The posting of this software on the web in January 2000 led to a lawsuit by major movie studios against its author. After a series of cases, courts finally ruled that the use of DeCSS violated the DMCA's anticircumvention provisions.

Title II provides "safe harbors" for Internet service providers (ISPs) whose customers/subscribers might be breaking copyright laws by downloading, posting, storing, or sending copyrighted material via its services. If an ISP has knowledge of infringing material and fails to take action to remove the material, it is not protected by the safe harbor measures. The ISP must also comply with clearly defined "notice and takedown" procedures that grant copyright holders a quick and simple way to halt access to allegedly infringing content. Copyright holders are granted the right to issue subpoenas to alleged copyright holders identified through their ISP. Title II of the DMCA also provides defined procedures for ISP users to challenge improper takedowns.

In March 2014, Viacom (owner of cable networks Comedy Central, MTV, and Nickelodeon as well as Paramount Studios) and Google ended a seven-year $1 billion copyright lawsuit involving YouTube, which is owned by Google. In the lawsuit, Viacom alleged that Google should be held responsible for the copyright infringements committed by YouTube users who posted some 79,000 copyrighted videos on its website between 2005 and 2008. Viacom argued that YouTube should have in place a means to monitor the content of videos being uploaded even though they were coming at the prodigious rate of more than 24 hours of viewing time per minute. YouTube countered that it had promptly complied with more than 100,000 takedown notices Viacom had sent it, thus adhering to the DMCA safe harbor procedures. Ultimately, the courts ruled that YouTube was covered by the "safe harbor" protections of the DMCA. Eventually Viacom and Google settled with no money changing hands.[22,23]

Because many copyright infringers take measures to conceal their true identity, copyright owners often must take additional steps if they wish to sue for copyright infringement. Provided a copyright owner has sent a DMCA notice, a John Doe subpoena can be obtained from a court clerk without even commencing a lawsuit. The subpoena compels the ISP to reveal the identity of the anonymous poster. The ISP is unlikely to resist the subpoena due to the associated legal costs.

The typical process for such lawsuits is that the IP addresses are collected for the alleged copyright violators. Attorneys then file a John Doe complaint in federal court and request the court to issue subpoenas to all ISPs used by the defendants. The subpoenas compel the ISPs to provide the defendants' names and other contact information. The attorneys then contact the defendants to offer them the opportunity to settle out of court and thus avoid embarrassment and legal fees.

Some see the DMCA as a boon to the growth of the Internet and its use as a conduit for innovation and freedom of expression. Without the safe harbors that the DMCA provides, the risk of copyright liability would be so great as to seriously discourage ISPs from hosting and transmitting user-generated content. Others see the DMCA as extending too much power to copyright holders. They share the viewpoint of Verizon general counsel William P. Barr who stated in testimony before Congress that the "broad and promiscuous subpoena procedure" of the DMCA grants "truly breathtaking powers to anyone who can claim to be or represent a copyright owner; powers that Congress has not even bestowed on law enforcement and national security personnel."[24]

Patents

A **patent** is a grant of a property right issued by the U.S. Patent and Trademark Office (USPTO) to an inventor. A patent permits its owner to exclude the public from making, using, or selling a protected invention, and it allows for legal action against violators. Unlike a copyright, a patent prevents independent creation as well as copying. Even if someone else invents the same item independently and with no prior knowledge of the patent holder's invention, the second inventor is excluded from using the patented device without permission of the original patent holder. The rights of the patent are valid only in the United States and its territories and possessions.

There are six types of patents, with the two of main concern to information technology firms being the utility patent and the design patent.

A **utility patent** is "issued for the invention of a new and useful process, machine, manufacture, or composition of matter, or a new and useful improvement thereof, it generally permits its owner to exclude others from making, using, or selling the invention for a period of up to twenty years from the date of patent application filing, subject to the payment of maintenance fees."[25] According to the USPTO, approximately 90 percent of the patent documents issued in recent years have been utility patents.

A **design patent**, which is "issued for a new, original, and ornamental design embodied in or applied to an article of manufacture," permits its owner to exclude others from making, using, or selling the design in question.[26] Design patents issued from applications filed on or after May 13, 2015, are granted for a term of 15 years from the date of grant. Design patents issued from applications filed before May 13, 2015, were granted for a term of 14 years from the date of grant.

Figure 6-1 shows the number of utility and design patents applied for and granted in recent years with roughly half the patents applied for having been granted.[27]

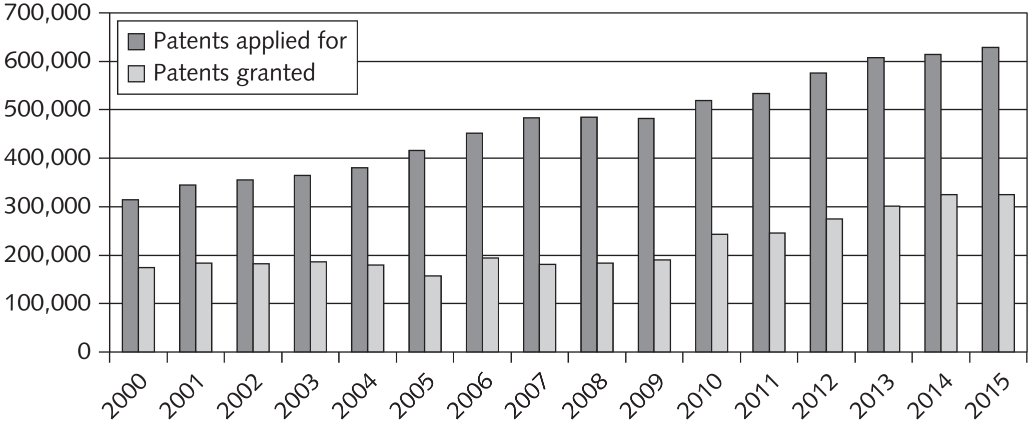


FIGURE 6-1 The number of utility and design patents applied for and granted (2000–2015)

Source: "U.S. Patent Activity Calendar Years 1790 to the Present," USPTO, https://www.uspto.gov/web/offices/ac/ido/oeip/taf/h_counts.htm, accessed January 18, 2017.

To obtain a U.S. patent, an application must be filed with the USPTO according to strict requirements. As part of the application, the USPTO searches the **prior art**—the existing body of knowledge available to a person of ordinary skill in the art—starting with patents and published material that have already been issued in the same area. The USPTO will not issue a patent for an invention whose professed improvements are already present in the prior art. Although the USPTO employs around 9,000 patent examiners to research the originality of each patent application, the average time from filing until the application is issued as a patent, rejected, or abandoned by the applicant is around

25 months. At the end of December 2016, there was a backlog of 550,000 unexamined patent applications.[28] Such delays in getting patents approved can be costly for companies that want to bring patented products to market quickly. As a result, in many cases, people trained in the patent process, rather than the inventors themselves, prepare patent applications.

The main body of law that governs patents is contained in Title 35 of the U.S. Code. Section 101 of the code states that "whoever invents or discovers any new or useful process, machine, manufacture or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor." Section 102 defines "novelty" as a necessary condition to grant a patent and describes various kinds of prior art that can be used as evidence that the invention is not novel. Section 103 describes "nonobviousness" as another mandatory requirement for a patent. To be patentable, an invention must not be obvious to a person having ordinary skill in the field on which the invention is based.

The U.S. Supreme Court has ruled that three classes of items cannot be patented: abstract ideas, laws of nature, and natural phenomena. Standing on its own, mathematical subject matter is also not entitled to patent protection. Thus, Pythagoras could not have patented his formula for the length of the hypotenuse of a right triangle ($c^2 = a^2 + b^2$). The statute does not identify computer software, gene sequences, or genetically modified bacteria as patentable subject matter. However, these items have subsequently been determined to be patentable in various court rulings.

Patent infringement, or the violation of the rights secured by the owner of a patent, occurs when someone makes unauthorized use of another's patent. Unlike with copyright infringement, there is no specified dollar amount limitation on the monetary penalty if patent infringement is found. In fact, if a court determines that the infringement is intentional, it can award up to three times the amount of the damages claimed by the patent holder. The most common defense against patent infringement is a counterattack on the claim of infringement and the validity of the patent itself. Even if the patent is valid, the plaintiff must still prove that every element of a claim was infringed and that the infringement caused some sort of damage.

Organizations often license the right to make, use, or sell their patented inventions to other organizations. The patent holder organization retains ownership of the invention and earns royalty payments on future sales of the product in which the patented invention is used. The patent holder may grant an exclusive license to one individual company or several companies.

IBM obtained 8,088 patents in 2016, the 24th consecutive year it obtained more utility patents than any other company.[29] By some estimates, IBM's licensing of patents, trademarks, and copyrights generates somewhere between $200 million and $2 billion in annual revenue for the company. Another company that generates significant income from licensing its patents is Qualcomm, a U.S. multinational semiconductor and telecommunications equipment manufacturer whose inventions, which helped launch the mobile revolution, can be found in billions of devices around the world. Qualcomm generated $7.8 billion in licensing revenue in 2014, representing 30 percent of the company's overall revenue.[30]

Licensing relationships with a licensee can go bad, resulting in legal fees and additional problems. For example, Apple Inc. sued Qualcomm, alleging that Qualcomm leveraged its monopoly position as a manufacturer of baseband chips, a critical component used in cell phones, to seek "onerous, unreasonable and costly" terms for patents. Those terms required Apple to pay Qualcomm as much five percent of the average price of an iPhone. Qualcomm's payment stayed the same as Apple added elements that increased the iPhone's capabilities and price even though those enhancements had nothing to do with the Qualcomm chip. Apple also alleged that Qualcomm required it to use only Qualcomm chips in its iPhones, preventing it from switching to chips made by competitors such as Intel Corp. In addition, the complaint seeks $1 billion in rebate payments that Apple says Qualcomm withheld as reprisal for Apple's participation in an investigation by South Korea's antitrust regulators. That investigation resulted in Qualcomm being fined $853 million for alleged anticompetitive patent-licensing practices.[31]

Leahy-Smith America Invents Act (2011)

Passed in 2011, the **Leahy-Smith America Invents Act**, which amends Title 35 of the U.S. Code, represented a major change in the U.S. patent law. Under this law, the U.S. patent system changed from a "first-to-invent" to a "first-inventor-to-file" system effective from March 16, 2013. That means if two people file for a patent application on the same invention at approximately the same time, the first person to file with the USPTO will receive the patent, not necessarily the person who actually invented the item first.[32,33]

The America Invents Act also expanded the definition of prior art used to determine the novelty of an invention and whether it can be patented. For example, if something resembling your invention were on sale anywhere in the world before you filed for a patent, that item is now considered part of the prior art and could prevent you from obtaining a patent. Prior to the passing of this law, only items for sale within the United States were considered prior art. The America Invents Act makes it more difficult to obtain a U.S. patent.[34]

Software Patents

A software patent claims as its invention some feature or process embodied in instructions executed by a computer. The courts and the USPTO have changed their attitudes and opinions on the patenting of software over the years. Prior to 1981, the courts regularly turned down requests for such patents, giving the impression that software could not be patented.[35]

In the 1981 *Diamond v. Diehr* case, the Supreme Court granted a patent to Diehr, who had developed a process control computer and sensors to monitor the temperature inside a rubber mold. The USPTO interpreted the court's reasoning to mean that just because an invention used software did not mean that the invention could not be patented. Based on this ruling, courts have slowly broadened the scope of protection for software-related inventions.[36] As a result, during the 1980s and 1990s, the USPTO granted thousands of software-related patents per year. Application software, business software, expert systems, and system software were patented, along with such software processes as compilation routines, editing and control functions, and operating system techniques. Many patents were granted for business methods implemented in software.

Starting in the latter half of the 2000s, the courts have become more restrictive on the granting of software patents.[37] Some software experts think that too many software patents are being granted, and they believe that this inhibits new software development.[38] Indeed, each new software patent lawsuit adds to the costs and business risks associated with software development.

A foreign exchange transaction is a type of transaction that involves conversion of currency of one country into that of another. Settlement risk in a foreign exchange transaction is the risk that one party pays the currency it sold but does not receive the currency it bought. CLS is a U.S. financial institution that provides settlement services to its members in the foreign exchange market. Alice Corporation is an Australian company that owned U.S. patents related to a computerized trading platform that handles financial transactions in which a third party settles obligations between two others so as to eliminate the risk that only one party will pay its obligation. Alice's patents address settlement risk by using the third party as the guarantor. Alice sued and claimed infringement by CLS for using its patents in "a computerized trading platform for exchanging obligations in which a trusted third party settles obligations between a first and second party so as to eliminate 'settlement risk.'" The case eventually made its way to the U.S. Supreme Court, which reasoned that using a third party to eliminate settlement risk is a fundamental and prevalent practice (an abstract idea) used in our modern economy. In a unanimous decision, the Supreme Court held that patent law should not restrain abstract ideas that are the "building blocks of human ingenuity." All of Alice's claims for patent protection were ruled ineligible. Since this ruling in 2014, the percentage of business methods patents rejected by the USPTO has increased from 31 percent to nearly 82 percent.[39]

Cross-Licensing Agreements

Many large software companies have cross-licensing agreements in which each party agrees not to sue the other over patent infringements. For example, Apple and HTC battled for several years over various mobile phone-related patents, eventually leading the U.S. International Trade Committee (ITC) to ban imports of two models of the HTC mobile phone. Following that ruling by the ITC, the two companies agreed to a 10-year cross-licensing agreement that permits each party to license the other's current and future patents.[40] In 2016, IBM entered into cross-licensing arrangements with Western Digital covering some 100 patents in the area of distributed storage systems and nonvolatile memory devices. In 2014, Twitter acquired 900 IBM patents, and in 2011, Google acquired more than 2,000 IBM patents in cross-licensing deals.[41]

Major IT firms usually have little interest in cross-licensing with smaller firms. As a result, small businesses must pay an additional cost from which many larger companies are exempt. Furthermore, small businesses are generally unsuccessful in enforcing their patents against larger companies. Should a small business bring a patent infringement suit against a large firm, the larger firm can overwhelm the small business with multiple patent suits, whether they have merit or not. Considering that the average patent lawsuit costs $3 to $10 million and takes two to three years to litigate, a small firm often simply cannot afford to fight; instead, it usually settles and licenses its patents to the large company.[42]

TRADE SECRETS

A trade secret is defined as business information that represents something of economic value, has required effort or cost to develop, has some degree of uniqueness or novelty, is generally unknown to the public, and is kept confidential.

Trade secret protection begins by identifying all the information that must be protected—from undisclosed patent applications to market research and business plans—and developing a comprehensive strategy for keeping the information secure. Trade secret law protects only against the *misappropriation* of trade secrets. If competitors come up with the same idea on their own, it is not misappropriation; in other words, the law doesn't prevent someone from using the same idea if it was developed independently.

Trade secret laws protect more technology worldwide than patent laws do, in large part because of the following key advantages:

- There are no time limitations on the protection of trade secrets, as there are with patents and copyrights.
- There is no need to file an application, make disclosures to any person or agency, or disclose a trade secret to outsiders to gain protection. (After the USPTO issues a patent, competitors can obtain a detailed description of it.) Hence, no filing or application fees are required to protect a trade secret.
- Although patents can be ruled invalid by the courts, meaning that the affected inventions no longer have patent protection, this risk does not exist for trade secrets.

Trade Secret Laws

Trade secret protection laws vary greatly from country to country. For example, the Philippines provides no legal protection for trade secrets. In some European countries, pharmaceuticals, methods of medical diagnosis and treatment, and information technology cannot be patented. Many Asian countries require foreign corporations operating there to transfer rights to their technology to locally controlled enterprises. (Coca-Cola reopened its operations in India in 1993 after halting sales for 16 years to protect the "secret formula" for its soft drink, even though India's vast population represented a huge potential market.) American businesses that seek to operate in foreign jurisdictions or enter international markets must take these differences into account. The misappropriation of trade secrets is estimated to cost U.S. companies somewhere between $160 billion and $480 billion each year.[43]

Uniform Trade Secrets Act

The **Uniform Trade Secrets Act (UTSA)** was drafted in the 1970s to bring uniformity to all the United States in the area of trade secret law. The first state to enact the UTSA was Minnesota in 1981, followed by 39 more states and the District of Columbia. The UTSA defines a *trade secret* as "information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

- Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by, persons who can obtain economic value from its disclosure or use, and
- Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

Under these terms, computer hardware and software can qualify for trade secret protection by the UTSA.[44]

The Economic Espionage Act

The **Economic Espionage Act (EEA) of 1996** (18 U.S. Code § 183) imposes penalties of up to $10 million and 15 years in prison for the theft of trade secrets. Before the

EEA, there was no specific criminal statute to help law enforcement agencies pursue economic espionage; the FBI was investigating nearly 800 such cases in 23 countries when the EEA was enacted.[45] The Commission on the Theft of American Intellectual Property has estimated that the impact of international intellectual property theft on U.S. businesses is hundreds of billions of dollars. In addition, it has cost the U.S. economy millions of jobs and diminished the incentive to innovate, thus lessening productivity growth and improvements in the quality of life.[46] As with the UTSA, information is considered a trade secret under the EEA only if companies take steps to protect it.

Defend Trade Secrets Act of 2016

The **Defend Trade Secrets Act of 2016** (DTSA) (Public Law No.: 114-153) amended the EEA to create a federal civil remedy for trade secret misappropriation. Prior to its enactment, civil claims for trade secret misappropriation were primarily governed by state law. In one such case, Sergey Aleynikov was found guilty under New York state law of theft of trade secrets. Aleynikov—a Goldman Sachs programmer who left the firm in 2007 to take a job paying $1.2 million annually with Teza Technologies, a group of widely recognized experts in quantitative trading—admitted copying Goldman's high-frequency trading code before he resigned but claimed the files were intended only as research for his new job. His initial convictions under the EEA were reversed after Aleynikov spent a year in federal prison; however, new charges brought in New York state court resulted in Aleynikov being found guilty of the unlawful use of secret scientific material under New York's penal code (Section 165.07). Aleynikov could be sentenced to up to four years in prison. Although Aleynikov was found guilty under New York state law, the wide variety in state statues governing trade secret misappropriation prior to the passage of DTSA created great uncertainty in the application of trade secret law across the United States.[47]

DTSA broadly defines misappropriation to include disclosure or use of a trade secret without express or implied consent or acquisition of a trade secret by anyone with reason to know the trade secret was acquired by theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means. However, reverse engineering and independent derivation are not considered improper. The act also allows for seizure of property under certain conditions to prevent dissemination of the misappropriated trade secret.[48]

One of the first lawsuits brought under the DTSA was against a high-level Monsanto employee who loaded 52 files of trade secret information onto his computer just before leaving the company for other employment. Under the DTSA, Monsanto was able to obtain a temporary restraining order requiring him to return all trade secret information he had acquired from Monsanto and prohibiting him from using or disclosing any misappropriated trade secrets.[49]

Employees and Trade Secrets

Employees are the greatest threat to the loss of company trade secrets—they might accidentally disclose trade secrets or steal them for monetary gain. Organizations must educate employees about the importance of maintaining the secrecy of corporate information.

Trade secret information should be labeled clearly as confidential and should only be accessible by a limited number of people. Most organizations have strict policies regarding nondisclosure of corporate information.

Because organizations can risk losing trade secrets when key employees leave, they often try to prohibit employees from revealing secrets by adding **nondisclosure clauses** to employment contracts. Thus, departing employees cannot take copies of computer programs or reveal the details of software owned by the firm.

Defining reasonable nondisclosure agreements can be difficult, as seen in the following example involving Apple. In addition to filing hundreds of patents on iPhone technology, the firm put into place a restrictive nondisclosure agreement to provide an extra layer of protection. Many iPhone developers complained bitterly about the tough restrictions, which prohibited them from talking about their coding work with anyone not on the project team and even prohibited them from talking about the restrictions themselves. Eventually, Apple admitted that its nondisclosure terms were overly restrictive and loosened them for iPhone software that was already released.[50]

Another option for preserving trade secrets is to have an experienced member of the human resources department conduct an exit interview with each departing employee. A key step in the interview is to review a checklist that deals with confidentiality issues. At the end of the interview, the departing employee is asked to sign an acknowledgment of responsibility not to divulge any trade secrets.

Employers can also use noncompete agreements to protect intellectual property from being used by competitors when key employees leave. A **noncompete agreement** prohibits an employee from working for any competitors for a period of time, often one to two years. When courts are asked to settle disputes over noncompete agreements, they must weigh several factors. First, they must consider the reasonableness of the restriction and how it protects confidential and trade secret information of the former employer. Second, they must weigh the employee's right to work and seek employment in the area where the employee has gained skill, experience, and business contacts. The courts also consider geographic area and the length of time of the restriction in relation to the pace of change in the industry.

Most states only enforce such noncompete agreements to the extent required to shelter the employer's legitimate confidential business interests. However, there is a wide range of treatment on noncompete agreements among the various states. For example, Ohio is highly supportive of former employers enforcing noncompete agreements while noncompete agreements are not as strictly enforced in California.[51]

The following is an example of a typical, although not necessary legally binding, noncompete agreement:

> The employee agrees as a condition of employment that in the event of termination for any reason, he or she will not engage in a similar or competitive business for a period of two years, nor will he or she contact or solicit any customer with whom Employer conducted business during his or her employment. This restrictive covenant shall be for a term of two years from termination, and shall encompass the geographic area within a 100-mile radius of Employer's place of business.

CRITICAL THINKING EXERCISE: AUTO REPAIR ELECTRONIC DATABASE

You and your friends are considering creating an electronic database that would contain all the information available to troubleshoot and repair every make and model of car from 2006 forward. The database would include do-it-yourself repair information, exploded schematics of automobile engines, wiring diagrams, recall information, and technical service bulletins, among other data. Subscribers would be able to enter the year, make, and model of a car along with a description of the problem and get all the information needed to work on that specific car. Most of the data would be scanned in from existing sources. Special software would be written to convert the user's problem description into a description recognized by the system's search engine, which would then generate queries to retrieve and present the most pertinent information to solve the problem. What intellectual property issues might you and your friends encounter in digitizing all these existing information? How might you be able to get around these issues? What means should you consider to protect your intellectual property?

CURRENT INTELLECTUAL PROPERTY ISSUES

This section discusses several issues that apply to intellectual property and information technology, including plagiarism, reverse engineering, open source code, competitive intelligence, trademark infringement, and cybersquatting.

Plagiarism

Plagiarism is the act of stealing someone's ideas or words and passing them off as one's own. The explosion of electronic content and the growth of the web have made it easy to cut and paste paragraphs into term papers and other documents without proper citation or quotation marks. To compound the problem, hundreds of online "paper mills" enable users to download entire term papers. Although some sites post warnings that their services should be used for research purposes only, many users pay scant heed. As a result, plagiarism has become an issue from elementary schools to the highest levels of academia. Plagiarism also occurs outside academia. Popular literary authors, playwrights, musicians, journalists, and even software developers have been accused of it.

Despite codes of ethics in place that clearly define plagiarism and prescribe penalties ranging from no credit on a paper to expulsion, many students still do not understand what constitutes plagiarism. Some students believe that all electronic content is in the public domain, while other students knowingly commit plagiarism either because they feel pressure to achieve a high GPA or because they are too lazy or pressed for time to do original work.

A recent survey reported that 55 percent of university presidents felt that plagiarism has increased over the past decade in spite of increased efforts to combat the practice.[52] Plagiarism by students taking free online courses from Coursea has become so widespread that one professor felt compelled to post a request for his 39,000 students to stop the practice after many of the students complained about their fellow students.[53]

Some instructors say that being familiar with a student's style of writing, grammar, and vocabulary enables them to determine if the student actually wrote a paper. In addition, plagiarism detection systems (see Table 6-2) allow teachers, corporations, law firms, and publishers to check for matching text in different documents as a means of identifying potential plagiarism.

TABLE 6-2 Partial list of plagiarism detection services and software

Name of service	Website	Provider
iThenticate	www.ithenticate.com	iParadigms
Turnitin	www.turnitin.com	iParadigms
SafeAssign	www.safeassign.com	Blackboard
Glatt Plagiarism Services	www.plagiarism.com	Glatt Plagiarism Services

Turnitin, a software product developed by California-based iParadigms, supports 15 languages and is used by over 10,000 educational institutions around the world. It uses three primary databases for content matching with over 58 billion web pages, some 570 million archived student papers, and 150 million articles from over 110,000 journals, periodicals, and books.[54] iThenticate is available from the same company that created Turnitin, but it is designed to meet the needs of members of the information industry, such as publishers, research facilities, legal firms, government agencies, and financial institutions.[55]

Interestingly, four high school students brought a lawsuit against iParadigms, accusing the firm of copyright infringement. The basis of their lawsuit was that the firm's primary product, Turnitin, used archived student papers without their permission to assess the originality of newly submitted papers. However, both a district court and a court of appeals ruled that the use of student papers for purposes of plagiarism detection constitutes fair use and is therefore not a copyright infringement. A U.S. court of appeals ruled that such use of student papers "has a protective effect" on the future marketability of the students' works and "provides a substantial public benefit through the network of institutions using Turnitin."[56]

The following list shows some of the actions that schools can take to combat student plagiarism:

- Help students understand what constitutes plagiarism and why they need to cite sources properly.
- Show students how to document web pages and materials from online databases.
- Schedule major writing assignments so that portions are due over the course of the term, thus reducing the likelihood that students will get into a time crunch and be tempted to plagiarize to meet the deadline.
- Make clear to students that instructors are aware of Internet paper mills.
- Ensure that instructors both educate students about plagiarism detection services and make them aware that they know how to use these services.
- Incorporate detection software and services into a comprehensive antiplagiarism program.

Plagiarism can also be an issue in the field of software development. Measure of Software Similarity (MOSS) is software used to measure the similarities among computer programs written in languages such as Ada, C, C++, Java, Lisp, and Paschal. MOSS is used to detect plagiarism in computer programming classes and commercial software.

Reverse Engineering

Reverse engineering is the process of taking something apart in order to understand it, build a copy of it, or improve it. It was originally applied to computer hardware but is now commonly applied to software as well. Reverse engineering of software involves analyzing it to create a new representation of the system in a different form or at a higher level of abstraction. Often, reverse engineering begins by extracting design-stage details from program code. Design-stage details about an information system are more conceptual and less defined than the program code of the same system. Microsoft has been accused repeatedly of reverse engineering products—ranging from the Apple Macintosh user interface to many Apple operating system utility features that were incorporated into DOS (and later Windows), to early word-processing and spreadsheet programs that set the design for Word and Excel, to Google's methods for improving search results for its Bing search engine.[57]

One frequent use of reverse engineering for software is to modify an application that ran on one vendor's database so that it can run on another's (e.g., from Access to Oracle). Database management systems use their own programming language for application development. As a result, organizations that want to change database vendors are faced with rewriting existing applications using the new vendor's database programming language. The cost and length of time required for this redevelopment can deter an organization from changing vendors and deprive it of the possible benefits of converting to an improved database technology.

Using reverse engineering, a developer can use the code of the current database programming language to recover the design of the information system application. Next, code-generation tools can be used to take the design and produce code (forward engineer) in the new database programming language. This reverse-engineering and code-generating process greatly reduces the time and cost needed to migrate the organization's applications to the new database management system. No one challenges the right to use this process to convert applications developed in-house. After all, those applications were developed and are owned by the companies using them. It is quite another matter, however, to use this process on a purchased software application developed and licensed by outside parties. Most IT managers would consider this action unethical because the software user does not actually own the right to the software. In addition, a number of intellectual property issues would be raised, depending on whether the software was licensed, copyrighted, or patented.

Other reverse-engineering issues involve tools called compilers and decompilers. A compiler is a language translator that converts computer program statements expressed in a source language (such as Java, C, C++, and COBOL) into machine language (a series of binary codes of 0s and 1s) that the computer can execute. When a software manufacturer provides a customer with its software, it usually provides the software in machine-language form. Tools called reverse-engineering compilers, or decompilers, can read the machine language and produce the source code. For example, Reverse Engineering Compiler (REC) is a decompiler that reads an executable, machine-language file and produces a C-like representation of the code used to build the program.

Decompilers and other reverse-engineering techniques can be used to reveal a competitor's program code, which can then be used to develop a new program that either duplicates the original or interfaces with the program. Thus, reverse engineering provides a way to gain access to information that another organization may have copyrighted or classified as a trade secret.

The courts have ruled in favor of using reverse engineering to enable interoperability. In the early 1990s, video game maker Sega developed a computerized lock so that only Sega video cartridges would work on its entertainment systems. This essentially shut out competitors from making software for the Sega systems. *Sega Enterprises Ltd. v. Accolade, Inc.* dealt with rival game maker Accolade's use of a decompiler to read the Sega software source code. With the code, Accolade could create new software that circumvented the lock and ran on Sega machines. An appeals court ultimately ruled that if someone lacks access to the unprotected elements of an original work and has a "legitimate reason" for gaining access to those elements, disassembly of a copyrighted work is considered to be a fair use under section 107 of the Copyright Act. The unprotected element in this case was the code necessary to enable software to interoperate with the Sega equipment. The court reasoned that to refuse someone the opportunity to create an interoperable product would allow existing manufacturers to monopolize the market, making it impossible for others to compete. This ruling had a major impact on the video game industry, allowing video game makers to create software that would run on multiple machines.

Software license agreements increasingly forbid reverse engineering. As a result of the increased legislation affecting reverse engineering, some software developers are moving their reverse-engineering projects offshore to avoid U.S. rules.

The ethics of using reverse engineering are debated. Some argue that its use is fair if it enables a company to create software that interoperates with another company's software or hardware and provides a useful function. This is especially true if the software's creator refuses to cooperate by providing documentation to help create interoperable software. From the consumer's standpoint, such stifling of competition increases costs and reduces business options. Reverse engineering can also be a useful tool in detecting software bugs and security holes.

Others argue strongly against the use of reverse engineering, saying it can uncover software designs that someone else has developed at great cost and taken care to protect. Opponents of reverse engineering contend it unfairly robs the creator of future earnings and significantly reduces the business incentive for software development.

Open Source Code

Historically, the makers of proprietary software have not made their source code available, but not all developers share that philosophy. **Open source code** is any program whose source code is made available for use or modification, as users or other developers see fit. The basic premise behind open source code is that when many programmers can read, redistribute, and modify a program's code, the software improves. Programs with open source code can be adapted to meet new needs, and bugs can be rapidly identified and fixed. Open source code advocates believe that this process produces better software than the traditional closed model.

A considerable amount of open source code is available, and an increasing number of organizations use open source code. For example, much of the Internet runs on open source code; when you access a web page, send a text, or post a status update, you are likely using an open source program such as Linux, Apache HTTP, PHP, Perl, Python, or Ruby.[58]

A common use of open source software is to move data from one application to another and to extract, transform, and load business data into large databases. Two frequently cited reasons for using open source software are that it provides a better solution to a specific business problem and that it costs less. Open source software is used in applications developed for Apple's iPhone, Android smartphones, and other mobile devices. See Table 6-3 for a partial listing of commonly used open source software.

TABLE 6-3 Commonly used open source software

Open source web browsers	Open source database management systems	Open source accounting applications
Chrome	MySQL	GnuCash
Firefox	PostgreSQL	SQL Ledger
Opera	SQLite	X Tuple PostBooks
Chromium	MongoDB	Compiere
Midori	Cubrid	Turbo Cash
QupZilla	MariaDB	KashFlow

Reasons that firms or individual developers create open source code, even though they do not receive money for it, include the following:

- Some people share code to earn respect for solving a common problem in an elegant way.
- Some people have used open source code that was developed by others and feel the need to pay back by helping other developers.
- A firm may be required to develop software as part of an agreement to address a client's problem. If the firm is paid for the employees' time spent to develop the software rather than for the software itself, it may decide to license the code as open source and use it either to promote the firm's expertise or as an incentive to attract other potential clients with a similar problem.
- A firm may develop open source code in the hope of earning software maintenance fees if the end user's needs change in the future.
- A firm may develop useful code but may be reluctant to license and market it, and so might donate the code to the general public.

There are various definitions of what constitutes open source code, each with its own idiosyncrasies. The GNU General Public License (GPL) was a precursor to the open source code defined by the Open Source Initiative (OSI). GNU is a computer operating system comprised entirely of free software; its name is a recursive acronym for GNUs Not Unix. The GPL is intended to protect GNU software from being made proprietary, and it lists terms and conditions for copying, modifying, and distributing free software. The OSI is a nonprofit organization that advocates for open source and certifies open source licenses. Its certification mark, "OSI Certified," may be applied only to software distributed under an open source license that meets OSI criteria, as described at its website, *www.opensource.org*.

A software developer could attempt to make a program open source simply by putting it into the public domain with no copyright. This would allow people to share the program and their improvements, but it would also allow others to revise the original code and then distribute the resulting software as their own proprietary product. Users who received the program in the modified form would no longer have the freedoms associated with the original software. Use of an open source license avoids this scenario.

Competitive Intelligence

Competitive intelligence is legally obtained information that is gathered to help a company gain an advantage over its rivals. For example, some companies have employees who monitor the public announcements of property transfers to detect any plant or store expansions of competitors. An effective competitive intelligence program requires the continual gathering, analysis, and evaluation of data with controlled dissemination of useful information to decision makers. Competitive intelligence is often integrated into a company's strategic plan and executive decision making.

Competitive intelligence is not the same as **industrial espionage**, which is the use of illegal means to obtain business information not available to the general public. In the United States, industrial espionage is a serious crime that carries heavy penalties.

Almost all the data needed for competitive intelligence can be collected from examining published information or interviews, as outlined in the following list:

- 10-K or annual reports
- An SC 13D acquisition—a filing by shareholders who report owning more than five percent of common stock in a public company
- 10-Q or quarterly reports
- Press releases
- Promotional materials
- Websites
- Analyses by the investment community, such as a Standard & Poor's stock report
- Dun & Bradstreet credit reports
- Interviews with suppliers, customers, and former employees

- Calls to competitors' customer service groups
- Articles in the trade press
- Environmental impact statements and other filings associated with a plant expansion or construction
- Patents

By coupling this competitive intelligence data with analytical tools and industry expertise, an experienced analyst can make deductions that lead to significant information. According to Avinash Kaushik, self-described "analytics evangelist" for Google, "The Web is the best competitive intelligence tool in the world." Kaushik likens the failure to use such data to driving a car 90 miles an hour with the windshield painted black, then scraping off the paint and realizing "you're going 90 but everyone else is going 220, and you're going to die."

A wide array of software applications, databases, and social media tools are available for companies—and individuals—looking for competitive intelligence data, including the following:

- Rapportive is software that can be added to your email application or web browser to provide you with rich contact profiles that show you what people look like, where they are based, and what they do. Such information can help you build rapport quickly by enabling you to mention shared interests.
- Crunchbase is a free database of technology of over 110,000 companies, people, and investors.
- CORI (*http://cori.missouri.edu/pages/ksearch.htm*) is an online database of more than 690,000 contract documents, most of which are executed agreements made public through SEC and other regulatory agency filings; users can access the database using a full-text search and retrieval system.
- ThomasNet.com is an excellent source for identifying suppliers and sources for products.
- WhoGotFunded.com is a comprehensive website of data about what organizations have received funding and for what purposes.

Competitive intelligence gathering has become enough of a science that over two dozen colleges and universities offer courses or even entire programs in this subject. Also, the Strategic and Competitive Intelligence Professionals organization (*www.scip.org*) offers ongoing training programs and conferences.

Without proper management safeguards, the process of gathering competitive intelligence can cross over to industrial espionage and dirty tricks. One frequently used dirty trick is to enter a bar near a competitor's plant or headquarters, strike up a conversation, and ply people for information after their inhibitions have been weakened by alcohol.

Competitive intelligence analysts must avoid unethical or illegal actions, such as lying, misrepresentation, theft, bribery, or eavesdropping with illegal devices. Table 6-4 provides a manager's checklist for running an ethical competitive intelligence operation. The preferred answer to each question in the checklist is *yes.*

TABLE 6-4 A manager's checklist for running an ethical competitive intelligence operation

Question	Yes	No
Has the competitive intelligence organization developed a mission statement, objectives, goals, and a code of ethics?		
Has the company's legal department approved the mission statement, objectives, goals, and code of ethics?		
Do analysts understand the need to abide by their organization's code of ethics and corporate policies?		
Is there a rigorous training and certification process for analysts?		
Do analysts understand all applicable laws—domestic and international—including the Uniform Trade Secrets Act, Defend Trade Secrets Act, and the Economic Espionage Act, and do they understand the critical importance of abiding by them?		
Do analysts disclose their true identity as well as the name of their organization prior to any interviews?		
Do analysts understand that everything their firm learns about the competition must be obtained legally?		
Do analysts respect all requests for anonymity and confidentiality of information?		
Has the company's legal department approved the processes for gathering data?		
Do analysts provide honest recommendations and conclusions?		
Is the use of third parties to gather competitive intelligence carefully reviewed and managed?		

Trademark Infringement

A **trademark** is a logo, package design, phrase, sound, or word that enables a consumer to differentiate one company's products from another's. Consumers often cannot examine goods or services to determine their quality or source, so instead they rely on the labels attached to the products. The Lanham Act of 1946 (also known as the Trademark Act, Title 15, of the U.S. Code) defines the use of a trademark, the process for obtaining a trademark from the USPTO, and the penalties associated with trademark infringement. The law gives the trademark's owner the right to prevent others from using the same mark or a confusingly similar mark on a product's label.

The United States has a federal system that stores trademark information; merchants can consult this information to avoid adopting marks that have already been taken. Merchants seeking trademark protection apply to the USPTO if they are using the mark in interstate commerce or if they can demonstrate a true intent to do so. Trademarks can be renewed forever—as long as a mark is in use.

It is not uncommon for an organization that owns a trademark to sue another organization over the use of that trademark in a website or a domain name. The court rulings in such cases are not always consistent and are quite difficult to judge in advance.

Nominative fair use is a defense often employed by the defendant in trademark infringement cases in which a defendant has used a plaintiff's mark to identify the plaintiff's products or services in conjunction with its own product or services. To successfully employ this defense, the defendant must show three things:[59]

- that the plaintiff's product or service cannot be readily identifiable without using the plaintiff's mark,
- that it uses only as much of the plaintiff's mark as necessary to identify the defendant's product or service, and
- that the defendant does nothing with the plaintiff's mark that suggests endorsement or sponsorship by the plaintiff.

This defense was first applied to websites in *Playboy Enterprises, Inc. v. Terri Welles.* Welles was the Playboy™ Playmate of the Year™ in 1981. In 1997, she created a website to offer free photos of herself, advertise the sale of additional photos, solicit memberships in her photo club, and promote her spokeswoman services. Welles used the trademarked terms and *Playmate of the Year* to describe herself on her website. The Ninth Circuit Court of Appeals determined that the former Playboy model's use of trademarked terms was permissible, nominative use. By using the nominative fair use defense, Welles avoided a motion for preliminary injunction, which would have restrained her from continuing to use the trademarked terms on her website.[60]

IGB Eletronica is a Brazilian telecommunications firm that designs and markets various consumer electronics products, including smartphones, for the Brazilian market. In 2000, the firm petitioned the Brazilian Industrial Property Institute (INPI) for the exclusive rights to the product name "iPhone." IGB was finally granted rights to the name in 2008, by coincidence, the same year that Apple's first iPhone was released. IGB released the Gradiente iPhone, which runs the Android operating system, in 2012, just a month before the trademark was to expire. Apple initiated a lawsuit over IGB's use of the iPhone. Initially, Brazil's INPI ruled in favor of IGB's finding that Apple had no right to use the iPhone name in the country. Apple then appealed that decision. The judge ruled that giving the Gradiente phone exclusive rights to the name would be unfair to Apple since "all the (Apple) product's renown and client following have been built on its performance and excellence as a product."[61] Thus, the two firms have the right to use the iPhone name in Brazil.

Cybersquatting

Companies that want to establish an online presence know that the best way to capitalize on the strengths of their brand names and trademarks is to make the names part of the domain names for their websites. When websites were first established, there was no procedure for validating the legitimacy of requests for website names, which were given out on a first-come, first-served basis. And in the early days of the web, many **cybersquatters** registered domain names for famous trademarks or company names to which they had no connection, with the hope that the trademark's owner would eventually buy the domain name for a large sum of money.

The main tactic organizations use to circumvent cybersquatting is to protect a trademark by registering numerous domain names and variations as soon as the organization knows it wants to develop a web presence (e.g., UVXYZ.com, UVXYZ.org, and UVXYZ.info). In addition, trademark owners who rely on non-English-speaking customers often register their names in multilingual form. Registering additional domain names is far less expensive than attempting to force cybersquatters to change or abandon their domain names.

Other tactics can also help curb cybersquatting. For example, the Internet Corporation for Assigned Names and Numbers (ICANN) is a nonprofit corporation responsible for managing the Internet's domain name system. Prior to 2000, eight generic top-level domain names were in existence: .com, .edu, .gov, .int, .mil, .net, .org, and .arpa. In 2000, ICANN introduced seven more: .aero, .biz, .coop, .info, .museum, .name, and .pro. In 2004, ICANN introduced .asia, .cat, .mobi, .tel, and .travel. The generic top-level domain .xxx was approved in 2011. With each new round of generic top-level domains, current trademark holders are given time to assert rights to their trademarks in the new top-level domains before registrations are opened up to the general public. As of March 2016, there were 882 top-level domain names, which can be found at *http://blog.europeandomaincentre.com/list-of-domain-extensions/#*.

ICANN also has a Uniform Domain-Name Dispute-Resolution Policy, under which most types of trademark-based domain name disputes must be resolved by agreement, court action, or arbitration before a registrar will cancel, suspend, or transfer a domain name. The ICANN policy is designed to provide for the fast, relatively inexpensive arbitration of a trademark owner's complaint that a domain name was registered or used in bad faith.

The Anticybersquatting Consumer Protection Act (ACPA), enacted in 1999, allows trademark owners to challenge foreign cybersquatters who might otherwise be beyond the jurisdiction of U.S. courts. Also under this act, trademark holders can seek civil damages of up to $100,000 from cybersquatters that register their trade names or similar-sounding names as domain names. The act also helps trademark owners challenge the registration of their trademark as a domain name even if the trademark owner has not created an actual website.

In 1994, a reporter bought the mcdonalds.com domain for a story he was writing for *Wired* magazine about the value of domain names. At this very early stage of the Internet, nobody at McDonald's saw any value to being online. Eventually McDonald's realized their mistake and wanted to use the domain name. So the author persuaded the company to make a charitable contribution of $3,500 to a public school to provide computers and Internet access in exchange for returning the domain name to McDonalds.[62]

CRITICAL THINKING EXERCISE: NONCOMPETE CLAUSE

Silicon Beach, an area on the west side of the Los Angeles metropolitan area, is home to some 500 tech startup companies. Major technology companies that have opened offices in the region include AOL, BuzzFeed, Electronic Arts, Facebook, Google, Hulu, Salesforce, Yahoo, and YouTube. You are a member of the human resources organization of a Silicon Beach tech company. Your boss has asked you to prepare a recommendation on implementing a noncompete clause in the employment contract for all new hires. Would you support adding a noncompete clause for your company's new hires? Why or why not?

Summary

What does the term intellectual property encompass, and what measures can organizations take to protect their intellectual property?

- Intellectual property is a term used to describe works of the mind—such as art, books, films, formulas, inventions, music, and processes—that are distinct and owned or created by a single person or group.
- Copyrights, patents, trademarks, and trade secrets form a complex body of law relating to the ownership of intellectual property, which represents a large and valuable asset to most companies. If these assets are not protected, other companies can copy or steal them, resulting in significant loss of revenue and competitive advantage.
- A copyright is the exclusive right to distribute, display, perform, or reproduce an original work in copies; to prepare derivative works based on the work; to and grant these exclusive rights to others.
- Copyright infringement is a violation of the rights secured by the owner of a copyright. Infringement occurs when someone copies a substantial and material part of another's copyrighted work without permission.
- Copyright law has proven to be extremely flexible in covering new technologies, including software, video games, multimedia works, and web pages. However, evaluating the originality of a work can be difficult and disagreements over whether or not a work is original sometimes lead to litigation.
- Copyrights provide less protection for software than patents; software that produces the same result in a slightly different way may not infringe a copyright if no copying occurred.
- The fair use doctrine established four factors for courts to consider when deciding whether a particular use of copyrighted property is fair and can be allowed without penalty: (1) the purpose and character of the use, (2) the nature of the copyrighted work, (3) the portion of the copyrighted work used, and (4) the effect of the use on the value of the copyrighted work.
- The use of copyright to protect computer software raises many complicated issues of interpretation of what constitutes infringement.
- The Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008 increased trademark and copyright enforcement; it also substantially increased penalties for infringement.
- The original General Agreement on Tariffs and Trade (GATT), signed in 1993, created the World Trade Organization (WTO) in Geneva, Switzerland, to enforce compliance with the agreement. GATT includes a section covering copyrights called the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).
- The WTO is a global organization that deals with rules of international trade based on WTO agreements that are negotiated and signed by representatives of the world's trading nations The goal of the WTO is to help producers of goods and services, exporters, and importers conduct their business.
- The World Intellectual Property Organization (WIPO) is an agency of the United Nations dedicated to "the use of intellectual property as a means to stimulate innovation and creativity."

- The Digital Millennium Copyright Act (DMCA), which was signed into law in 1998, implements two WIPO treaties in the United States. The DMCA also makes it illegal to circumvent a technical protection or develop and provide tools that allow others to access a technologically protected work. In addition, the DMCA limits the liability of Internet service providers for copyright infringement by their subscribers or customers.
- Some view the DMCA as a boon to the growth of the Internet and its use as a conduit for innovation and freedom of expression. Others believe that the DMCA has given excessive powers to copyright holders.

- A patent is a grant of property right issued by the U.S. Patent and Trademark Office (USPTO) to an inventor that permits its owner to exclude the public from making, using, or selling a protected invention, and it allows for legal action against violators. A patent prevents copying as well as independent creation (which is allowable under copyright law).
- For an invention to be eligible for a patent, it must fall into one of three statutory classes of items that can be patented: (1) it must be useful, (2) it must be novel, and (3) it must not be obvious to a person having ordinary skill in the same field.
- A utility patent is "issued for the invention of a new and useful process, machine, manufacture, or composition of matter, or a new and useful improvement thereof." A design patent, which is "issued for a new, original, and ornamental design embodied in or applied to an article of manufacture," permits its owner to exclude others from making, using, or selling the design in question.
- Unlike copyright infringement, for which monetary penalties are limited to certain specified dollar amounts, if the court determines that a patent has been intentionally infringed, it can award up to triple the amount of the damages claimed by the patent holder.
- The Leahy-Smith America Invents Act changed the U.S. patent system from a "first-to-invent" to a "first-inventor-to file" system and expanded the definition of prior art, which is used to determine the novelty of an invention and whether it can be patented. The act made it more difficult to obtain a patent in the United States.
- The courts and the U.S. Patent and Trademark Office (USPTO) have changed their attitudes and opinions of the patenting of software over the years.
- To qualify as a trade secret, information must have economic value and must not be readily ascertainable. In addition, the trade secret's owner must have taken steps to maintain its secrecy. Trade secret laws do not prevent someone from using the same idea if it was developed independently or from analyzing an end product to figure out the trade secret behind it.
- Trade secrets are protected by the Uniform Trade Secrets Act, the Economic Espionage Act, and the Defend Trade Secrets Act, which amended the Economic Espionage Act to create a federal civil remedy for trade secret misappropriation.
- Trade secret law has three key advantages over the use of patents and copyrights in protecting companies from losing control of their intellectual property: (1) There are no time limitations on the protection of trade secrets, unlike patents and copyrights; (2) there is no need to file any application or otherwise disclose a trade secret to outsiders to gain protection; and (3) there is no risk that a trade secret might be found invalid in court.

- Because organizations can risk losing trade secrets when key employees leave, they often try to prohibit employees from revealing secrets by adding nondisclosure clauses to employment contracts. Employers can also use noncompete agreements to protect intellectual property from being used by competitors when key employees leave. A noncompete agreement prohibits an employee from working for any competitors for a period of time, often one to two years.

What are some of the current issues associated with the protection of intellectual property?

- Plagiarism is the act of stealing someone's ideas or words and passing them off as one's own. Plagiarism detection systems enable people to check the originality of documents and manuscripts.
- Reverse engineering is the process of breaking something down in order to understand it, build a copy of it, or improve it. It was originally applied to computer hardware but is now commonly applied to software.
- In some situations, reverse engineering might be considered unethical because it enables access to information that another organization may have copyrighted or classified as a trade secret.
- Recent court rulings and software license agreements that forbid reverse engineering, as well as restrictions in the DMCA, have made reverse engineering a riskier proposition in the United States.
- Open source code is any program whose source code is made available for use or modification, as users or other developers see fit. The basic premise behind open source code is that when many programmers can read, redistribute, and modify it, the software improves. Open source code can be adapted to meet new needs, and bugs can be rapidly identified and fixed.
- Competitive intelligence is legally obtained information that is gathered to help a company gain an advantage over its rivals. It is not the same as industrial espionage, which is the use of illegal means to obtain business information that is not readily available to the general public. In the United States, industrial espionage is a serious crime that carries heavy penalties.
- Competitive intelligence analysts must take care to avoid unethical or illegal behavior, including lying, misrepresentation, theft, bribery, or eavesdropping with illegal devices.
- A trademark is a logo, package design, phrase, sound, or word that enables a consumer to differentiate one company's products from another's. Website owners who sell trademarked goods or services must take care to ensure they are not sued for trademark infringement.
- Cybersquatters register domain names for famous trademarks or company names to which they have no connection, with the hope that the trademark's owner will eventually buy the domain name for a large sum of money.
- The main tactic organizations use to circumvent cybersquatting is to protect a trademark by registering numerous domain names and variations as soon as they know they want to develop a web presence.

Key Terms

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)

copyright

copyright infringement

cybersquatter

Defend Trade Secrets Act of 2016

design patent

Economic Espionage Act (EEA) of 1996

fair use doctrine

industrial espionage

intellectual property

Leahy-Smith America Invents Act

noncompete agreement

nondisclosure clauses

open source code

patent

patent infringement

plagiarism

prior art

Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008

reverse engineering

trademark

Uniform Trade Secrets Act (UTSA)

utility patent

Self-Assessment Questions

What does the term intellectual property encompass, and what measures can organizations take to protect their intellectual property?

1. Which of the following is not an example of intellectual property?
   a. A work of art
   b. An improvisational speech
   c. A trade secret of an organization
   d. A computer program
2. Patent law protects inventions, and ______________ law protects authored works.
3. Software can be protected under patent law, but it can also be copyright protected. True or False?
4. The courts may award up to triple damages for which of the following?
   a. Theft of trade secrets
   b. Copyright infringement
   c. Trademark infringement
   d. Patent infringement
5. Two software manufacturers develop separate but nearly identical programs for playing an online game. Even though the second manufacturer can establish that it developed the program on its own, without knowledge of the existing program, that manufacturer could be found guilty of patent infringement. True or False?
6. Title II of the ______________ amends the Copyright Act by adding a new section that enables a website operator that allows users to post content on its website to avoid copyright infringement if certain “safe harbor” provisions are followed.

7. A(n) ______________ is a logo, package design, phrase, sound, or word that enables a consumer to differentiate one company's products from another's.
8. Many large software companies have ______________ agreements with each other in which each agrees not to sue the other over patent infringement.
9. The ______________ doctrine established four factors for courts to consider when deciding whether a particular use of copyrighted property is fair and can be allowed without penalty.
10. A ______________ is a form of protection for intellectual property that does not require any disclosures or the filing of an application.
    a. copyright
    b. patent
    c. trade secret
    d. trademark
11. The Defend Trade Secrets Act amended the EEA to create a federal civil remedy for ______________.
    a. copyright infringement
    b. patent infringement
    c. trade secret misappropriation
    d. trademark infringement

What are some of the current issues associated with the protection of intellectual property?

12. Musicians, journalists, and even software developers have been accused of plagiarism. True or False?
13. The process of taking something apart in order to understand it, build a copy of it, or improve it is called ______________.
14. As part of the patent application, the USPTO searches the existing body of knowledge that is available to a person of ordinary skill in the art. This existing body of knowledge is also called ______________.
15. ______________ refers to any program whose source code is made available for use or modification, as users or other developers see fit.
16. The main tactic used to circumvent ______________ is to register numerous domain name variations as soon as an organization thinks it might want to develop a web presence.

Self-Assessment Answers

1. b; 2. copyright; 3. True; 4. d; 5. True; 6. Digital Millennium Copyright Act (DMCA); 7. trademark; 8. cross-licensing; 9. fair use; 10. c; 11. c; 12. True; 13. reverse engineering; 14. prior art; 15. Open source code; 16. cybersquatting

Discussion Questions

1. Do you believe that copyright, patent, and trade secret laws and their enforcement have accelerated the pace on innovation or slowed it? Explain your answer.
2. Explain the concept that an idea cannot be copyrighted, but the expression of an idea can be, and why this distinction is a key to understanding copyright protection.
3. Briefly discuss Titles I and II of the DMCA, including the primary protections it provides for copyrighted material as well as the associated penalties. Do you believe that the DMCA has given excessive powers to copyright holders? Why or why not?
4. Identify the necessary conditions to grant a patent according to Title 35 of the U.S. Code.
5. How did the Defend Trade Secrets Act modify U.S. trademark law? Do you think this act was an improvement over the preexisting patent protections? Why or why not?
6. What is a cross-licensing agreement? How do large hardware and software companies use such agreements? Do you think their use is fair to small technology firms? Why or why not?
7. Do you think that a high priority should be placed by the USPTO on doing whatever is necessary to reduce the backlog of patent applications in order to shorten the length of time required to obtain a patent application decision? Why or why not?
8. What is the role of the WTO, and what is the scope and intent of its TRIPS Agreement?
9. Briefly discuss how the courts and USPTO have changed their opinions and attitudes toward the patenting of software over the years. Do you believe that software patents inhibit new software development? Why or why not?
10. Identify and briefly discuss three key advantages that trade secret law has over the use of patents and copyrights in protecting intellectual property. Are there any drawbacks with the use of trade secrets to protect intellectual property?
11. What problems can arise in using nondisclosure and noncompete agreements to protect intellectual property?
12. Outline an approach that a university might take to successfully combat plagiarism by its students.
13. Under what conditions do you think that the use of reverse engineering is an acceptable business practice?
14. Why might an organization opt to produce open source code rather than focus on the creation of proprietary software?
15. What are the pros and cons of adopting open source code for use within an organization?
16. What measures can companies take to combat cybersquatting?

What Would You Do?

Use the five-step decision-making process discussed in to analyze the following situations and recommend a course of action.

1. You are a recruiter of IT talent for a headhunter firm. A senior manager from one of the major software development firms in the area is on the phone with you, demanding that you stop contacting her employees about job opportunities with competing firms. She explains

that senior executives at her firm all sign a noncompete clause as part of their employment contract. How do you respond?

2. You have been asked by the CEO of your software organization to hire and manage a small group of software developers in an attempt to reverse engineer the latest release of the software by your leading competitor. The goal of the group will be to identify features that could be implemented into the next few releases of your firm's software. Would you consider hiring software developers from your competitors to start this group? Why or why not? What sort of legal and/or ethical questions might be raised by this reverse engineering effort?

3. You have been promoted to the position of manager of your company's competitive intelligence organization. Senior management fired the previous manager because they felt he was too conservative in his approach to gathering information; they want someone who can "think outside the box." What ideas do you have about gathering competitive intelligence that would be effective, although perhaps somewhat unethical or illegal? Would you be willing to take these actions with senior management's encouragement?

4. You are interviewing for the role of human resources manager for a network hardware design and manufacturing firm. Over the last year, the firm has lost a number of high-level executives who left the firm to go to work for competitors. During the course of your interview, you are asked what measures you would put in place to reduce the potential loss of trade secrets from executives leaving the firm. How would you respond?

5. You have procrastinated too long and now your final paper for your junior Modern Middle Eastern history course is due in just five days—right in the middle of final exam week. The paper counts for half your grade for the term and would probably take you at least 20 hours to research and write. Your roommate, an English major from Saudi Arabia with a 3.8 GPA, has suggested two options: He will write an original paper for you for $100, or he will show you two or three "paper mill" websites, from which you can download a paper for less than $35. You want to do the right thing, but writing the paper will take away from the time you have available to study for your final exam in three other courses. What would you do?

6. You are the vice president for software development at a small, private firm. Sales of your firm's products have been strong, but you recently detected a patent infringement by one of your larger competitors. Your in-house legal staff has identified three options: (1) ignore the infringement out of fear that your larger competitor will file numerous countersuits; (2) threaten to file suit, but try to negotiate an out-of-court settlement for an amount of money that you feel your larger competitor would readily pay; or (3) point out the infringement and negotiate aggressively for a cross-licensing agreement with the competitor, which has numerous patents you had considered licensing. What are the pros and cons of each option? Which option would you pursue and why?

Cases

1. Target Hires Key Executive Away from Amazon

A retailer's supply chain includes the vendors that supply products, warehouses that store the product, distribution centers that deliver product to the retailers, and retailers who offer the product to the ultimate purchaser. An effective supply chain is crucial to any business and can result in lower costs, improved profitability, and greater customer satisfaction and loyalty.

Although Target continues to be a powerful player in the U.S. retail market, it has had an ongoing problem with out-of-stock product. Experts say a major cause of this problem is that Target's supply chain was designed for brick-and-mortar store operations and isn't able to handle the additional demand and complexities of online orders. CEO Brian Cornell has recognized this as a critical problem for the retailer, noting that "Target's growth hinges on our ability to enhance the fundamental aspects of our business, starting with the supply chain."

So when Target recently decided to upgrade its supply chain, it went after a seasoned executive—Arthur Valdez, a high-level employee at rival Amazon. During a 16-year career at the world's largest online retailer, Valdez had been promoted through a variety of supply chain positions of increasing responsibility. He eventually became vice president of operations, charged with expanding Amazon's international supply chain.

Valdez was offered the position of executive vice president of supply chain and logistics at Target, reporting to Chief Operating Officer John Mulligan. In a statement announcing Valdez's hire, Mulligan noted that "Arthur's leadership and experience will be a tremendous asset as we continue to drive improvements in end-to-end processes, including leveraging our almost 1,800 stores to deliver a seamless experience for our guests."

In the retail industry, however, as in many other industries, employers frequently file lawsuits over noncompete clauses as part of a strategy to protect trade secrets from walking out the door. And following Target's announcement, Amazon filed a lawsuit in Washington state court to keep Valdez from starting his new job with Target. The lawsuit also serves as both a delay tactic and a warning to other employees and rival employers.

Amazon pointed out that a noncompete agreement signed by Valdez prohibited him from working for any direct rival for 18 months following the end of his employment with Amazon. In addition, Amazon claimed that Valdez shared confidential information with Target about how Amazon handles orders and logistics during the peak holiday season. "Mr. Valdez cannot lead Target's supply chain operations without referencing confidential information learned and developed by him at Amazon," the company said in its suit. Amazon also asked the court to make Valdez pay its legal fees. Amazon's complaint explained that "Mr. Valdez knows, created, and implemented Amazon's most confidential strategies and metrics, including competitive analysis of Target and other similar competitors, in Amazon's supply chain and logistics operations." The complaint further explained that Valdez "developed intimate knowledge of the proprietary metrics and analytics" used by Amazon in its supply chain operations.

In response to the Amazon lawsuit, Target asserted that Valdez had not violated any agreement, and according to a Target spokeswoman, the retailer took "significant precautions to ensure that any proprietary information remains confidential." Target declared that Amazon's suit was without merit.

States vary in the degree to which they will enforce noncompete agreements. In the state of Washington, the courts use a three-factor test to determine if a noncompete agreement is reasonable. The courts consider (1) whether restraint is necessary for the protection of the business or good will of the employer, (2) whether the noncompete agreement imposes upon the employee any greater restraint than is reasonably necessary to secure the business of the employer or the good will thereof, and (3) whether the degree of injury to the public due to the loss of the service and skill of the employee warrants nonenforcement.

Rather than resort to a protracted court battle, Amazon opted to settle with Valdez, under the terms of a confidential agreement.

Critical Thinking Questions

1. Do you believe that this case met the three-factor test of the state of Washington to enforce the noncompete clause of Valdez's contract? Why or why not?
2. What settlement terms do you think would be fair to both Target and Amazon?
3. Do noncompete clauses in employment contracts encourage or discourage innovation? Explain your answer.

Sources: Kavita Kumar, "Target Hires Amazon Executive to Help Improve Supply Chain," *Star Tribune*, February 29, 2016, www.startribune.com/target-hires-amazon-executive-to-help-improve-supply-chain/370516391/; Phil Wahba, "Amazon Sues Star Exec Who Is Defecting to Target," *Fortune*, March 22, 2016, http://fortune.com/2016/03/22/amazon-target-lawsuit; Jeff Christensen, "Amazon's Lawsuit and Non-Compete Agreements for Executives," *Michigan Business & Entrepreneurial Law Review*, April 12, 2016, http://mbelr.org/amazons-lawsuit-and-non-compete-agreements-for-executives; Daniel B. Kline, "Can Amazon Stop Target from Learning Its Supply Chain Secrets?" *Motley Fool*, March 29, 2016, www.fool.com/investing/general/2016/03/29/can-amazon-stop-target-from-learning-its-supply-ch.aspx; Kavita Kumar, "Target Hires Another Former Amazon Employee to Work on Supply Chain," *Star Tribune*, August 9, 2016, www.startribune.com/target-hires-another-former-amazon-employee-to-work-on-supply-chain/389626331/.

2. Intellectual Property Fight over Virtual Reality Headset

The Oculus Rift is a virtual reality headset developed and manufactured by Oculus VR, a technology company founded in 2012 by Palmer Luckey. The Rift, released in March 2016, enables users to experience virtual tourism, play first-person shooter games, and participate in other highly realistic games. A powerful gaming desktop or laptop is required to run Oculus software titles and deliver detail-rich graphics to the two high-resolution displays.

Oculus VR was purchased by Facebook in March 2014 for $2 billion. Although Oculus VR positioned the Rift to become the dominant virtual reality headset in the gaming market, Facebook has much bigger plans for the developing technology. According to Facebook CEO Mark Zuckerberg, the company plans to "make Oculus a platform for many other experiences. Imagine enjoying a courtside seat at a game, studying in a classroom of students and teachers all over the world or consulting with a doctor face-to-face—just by putting on goggles in your home. This is really a new communication platform."

ZeniMax, founded in 1986, creates and publishes original interactive entertainment content for consoles, computers, and handheld/wireless devices. It has a number of operating divisions, including Bethesda Game Studios, Battle Cry Studios, and Tango Gameworks. ZeniMax's intellectual properties include *The Elder Scrolls*, an action role-playing game, and the popular *Doom* and *Quake* first-person shooter video games series, along with several other successful video game franchises.

ZeniMax filed a lawsuit just months after Facebook acquired Oculus, claiming that Oculus cofounder and Rift inventor Palmer Luckey, CTO John Carmack (a former high-level ZeniMax employee), and several other former ZeniMax employees who are now working at Oculus built the Rift based on millions of dollars' worth of ZeniMax's research and copyrighted code developed over the course of several years. ZeniMax alleged that the Rift device was "primitive" until Carmack made improvements based on his knowledge from his work at ZeniMax. The company raised the allegation that Carmack worked on Oculus software while still employed at ZeniMax with the hopes that the court would rule that ZeniMax owns that work, even if it is markedly different from code previously owned by ZeniMax.

Oculus denied the allegations, saying the lawsuit arose shortly after Facebook purchased the company because ZeniMax saw a "chance for a quick payout." Oculus claimed that its products do not contain a single line of ZeniMax code.

In February 2017, a jury in Dallas, Texas, awarded $500 million to ZeniMax after finding that Oculus cofounder Palmer Luckey, and by extension Oculus, failed to honor a nondisclosure agreement. However, the jury found that Oculus did not steal or misappropriate trade secrets as contended by ZeniMax. Oculus was ordered to pay $200 million for breaking the nondisclosure agreement and an additional $50 million for copyright infringement. Oculus and Luckey each must also pay $50 million for false designation of origin for lying about the origin of its products. Former Oculus CEO Brendan Iribe, who now leads a PC VR division within Facebook, must also pay $150 million for false designation.

Oculus, which plans to appeal the verdict, issued a statement following the ruling asserting that "Oculus products are built with Oculus technology. Our commitment to the long-term success of VR remains the same, and the entire team will continue the work they've done since day one, developing VR technology that will transform the way people interact and communicate."

Critical Thinking Questions

1. At the time of this writing, it is unclear what impact the verdict in this lawsuit this will have. Do research to see if this lawsuit had a negative impact on Facebook's forays into the world of virtual reality, the sale of Oculus Rift headsets, Facebook profits, and/or its stock price.
2. It is entirely possible that two programmers could write very similar code to solve the same simple problem—say a program to play tic-tac-toe. However, as the problem being addressed grows in size and complexity, the number of ways to code a solution also grows. This can create a temptation for one programmer to "paraphrase" ideas taken from another programmer's work, rather than writing original code. How might such "paraphrasing" be detected? Should paraphrasing of another's code be considered copyright or patent infringement? Why or why not?
3. Do research to learn the current status of the appeal of this lawsuit. Write a few brief paragraphs summarizing your findings as well as your feelings about this lawsuit.

Sources: Jay Yarow, "The Only Explanation of Facebook Buying Oculus for $2 Billion That Makes Any Sense," *Business Insider*, March 26, 2014, www.businessinsider.com/why-mark-zuckerberg-bought-oculus-for-2-billion-2014-3; Klint Finley, "That Whole Oculus Lawsuit Hinges on What Makes Code 'New'," *Wired*, January 20, 2017, https://www.wired.com/2017/01/whole-oculus-lawsuit-hinges-makes-code-new/; Selena Larson, "Facebook Loses $500 Million Oculus Lawsuit," *CNN Money*, February 2, 2017, http://money.cnn.com/2017/02/01/technology/zenimax-oculus-lawsuit-500-million/; Timothy Poon and Brian Crecente, "Oculus Lawsuit Ends with Half Billion Dollar Judgment Awarded to ZeniMax," *Polygon*, February 1, 2017, www.polygon.com/2017/2/1/14474198/oculus-lawsuit-verdict; Michelle Castillo, "Facebook Ordered to Pay $500 Million in Damages Over VR Suit," *CNBC*, February 1, 2017, www.cnbc.com/2017/02/01/facebook-loses-vr-case.html.

End Notes

[1] Phillip Elmer-DeWitt, “How Apple and Samsung Got to $548 Million,” *Fortune*, http://fortune.com/2015/12/05/samsung-apple-timeline-settlement, December 5, 2015.

[2] Ibid.

[3] Shara Tibken, “*Apple v. Samsung* Patent Trial Recap: How It All Turned Out (FAQ),” *CNET*, May 7, 2014, https://www.cnet.com/news/apple-v-samsung-patent-trial-recap-how-it-all-turned-out-faq/.

[4] Ibid.

[5] Seth Fiegerman, “Supreme Court Sides with Samsung in Apple Patent Case,” *CNN Tech*, December 6, 2016, http://money.cnn.com/2016/12/06/technology/samsung-apple-supreme-court/.

[6] 17 U.S.C. 17 § 102(a).

[7] “Sonny Bono Copyright Term Extension Act,” Copyright Extension, http://www.copyrightextension.com/page01.html (accessed February 27, 2017).

[8] *Eldred v. Ashcroft*, Legal Information Institute, www.law.cornell.edu/supct/search/display.html?terms=copyright&url=/supct/html/01-618.ZS.html (accessed January 15, 2017).

[9] Joseph C. Self, “The ‘My Sweet Lord’/’He’s So Fine’ Plagiarism Suit,” www.abbeyrd.net/mysweet.htm (accessed January 15, 2017).

[10] Lydia Hutchinson, “George Harrison’s ‘My Sweet Lord’ Copyright Case,” *Performing Songwriter*, February10, 2015, http://performingsongwriter.com/george-harrison-my-sweet-lord/.

[11] “17 USC Section 107—Limitations on Exclusive Rights: Fair Use,” www.law.cornell.edu/uscode/text/17/107 (accessed January 17, 2017).

[12] David Kravets, “Fair Use Prevails as Supreme Court Rejects Google Books Copyright Case,” *ars TECHNICA*, April 18, 2016, http://arstechnica.com/tech-policy/2016/04/fair-use-prevails-as-supreme-court-rejects-google-books-copyright-case/.

[13] “Circular 61 Copyright Registration for Computer Programs,” https://www.copyright.gov/circs/circ61.pdf (accessed January 17, 2017).

[14] *Oracle v. Google*, Electronic Frontier Foundation, https://www.eff.org/cases/oracle-v-google (accessed January 17, 2017).

[15] Joe Mullin, “Google Beats Oracle—Android Makes ‘Fair Use’ of Java APIs,” *ars TECHNICA*, May 26, 2016, http://arstechnica.com/tech-policy/2016/05/google-wins-trial-against-oracle-as-jury-finds-android-is-fair-use/.

[16] Joe Mullin, “Second *Oracle v. Google* Trial Could Lead to Huge Headaches for Developers,” *ars TECHNICA*, May 8, 2016, http://arstechnica.com/tech-policy/2016/05/round-2-of-oracle-v-google-is-an-unpredictable-trial-over-api-fair-use/.

[17] “PRO-IP Act: Annual Report FY2012,” United States Department of Justice, December 2012, www.justice.gov/dag/iptaskforce/proipact/doj-pro-ip-rpt2012.pdf.

[18] “Supporting Innovation, Creativity & Enterprise: Charting a Path Ahead,” https://www.whitehouse.gov/sites/default/files/omb/IPEC (accessed January 18, 2017).

[19] "What Is the WTO?" World Trade Organization, www.wto.org (accessed January 17, 2017).

[20] "TRIPS and Its Impact on Developing Countries," *Sci Dev Net*, www.scidev.net/global/policy-brief/trips-and-its-impact-on-developing-countries.html (accessed January 18, 2017).

[21] "What Is WIPO?" World Intellectual Property Organization, www.wipo.int/about-wipo/en/what_is_wipo.html (accessed January 17, 2017).

[22] Jonathan Stempel, "Google, Viacom Settle Landmark YouTube Lawsuit," *Reuters*, March 18, 2014, www.reuters.com/article/us-google-viacom-lawsuit-idUSBREA2H11220140318.

[23] Joe Silver, "Viacom and Google Settle $1 Billion YouTube Lawsuit," *ars TECHNICA*, March 18, 2014, http://arstechnica.com/tech-policy/2014/03/viacom-and-google-reach-settlement-in-long-running-youtube-lawsuit/.

[24] *Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks, Hearing Before the Senate Judiciary Committee*, Testimony of William Barr, executive vice president and general counsel, Verizon Communications, September 9, 2003, https://www.judiciary.senate.gov/imo/media/doc/barr_testimony_09_09_03.pdf (accessed February 27, 2017).

[25] "Types of Patents," USPTO, March 2016, https://www.uspto.gov/web/offices/ac/ido/oeip/taf/patdesc.htm.

[26] Ibid.

[27] "U.S. Patent Activity Calendar Years 1790 to the Present," USPTO, https://www.uspto.gov/web/offices/ac/ido/oeip/taf/h_counts.htm (accessed January 18, 2017).

[28] "Data Visualization Center: Patents Dashboard," USPTO, December 2016, https://www.uspto.gov/dashboards/patents/main.dashxml.

[29] "IBM Inventors Receive Record-Breaking 8,000+ U.S. Patents in 2016," IBM, https://www-03.ibm.com/press/us/en/pressrelease/51353.wss.

[30] Charles Babcock, "IBM Wields Cloud Patents for Defense, Profit," *InformationWeek*, August 5, 2015, www.informationweek.com/cloud/ibm-wields-cloud-patents-for-defense-profit/a/d-id/1321616.

[31] Tripp Mickle, "Apple Sues Qualcomm Over Licensing Practices," *Wall Street Journal*, January 20, 2016, www.wsj.com/articles/apple-sues-qualcomm-over-licensing-practices-1484944919.

[32] Mitchell S. Bigel, "America Invents Act Punishes U.S. Innovators," *Law Technology News*, February 26, 2013, www.law.com/jsp/lawtechnologynews/PubArticleFriendlyLTN.jsp?id=1202589501107.

[33] Nathan Hurst, "How the America Invents Act Will Change Patenting Forever," *Wired*, March 15, 2013, www.wired.com/design/?p=146445.

[34] See Bigel, 2013.

[35] "The History of Software Patents: From Benson, Flook, and Diehr to Bilski and *Mayo v. Prometheus*," *Bitlaw*, www.bitlaw.com/software-patent/history.html (accessed January 16, 2017).

[36] *Diamond v. Diehr*, 450 U.S. 175(1981), *BitLaw*, www.bitlaw.com/source/cases/patent/Diamond_v_Diehr.html (accessed February 21, 2013).

[37] "The History of Software Patents: From Benson, Flook, and Diehr to Bilski and *Mayo v. Prometheus*," *Bitlaw*, www.bitlaw.com/software-patent/history.html (accessed January 16, 2017).

[38] Timothy B. Lee, "The Supreme Court Should Invalidate Software Patents," *Forbes*, July 28, 2011.

[39] Austin Underhill, "Who Is Alice, and Why Is She Driving Patent Attorneys Mad as Hatters?" *Above the Law*, February 19, 2016, http://abovethelaw.com/2016/02/who-is-alice-and-why-is-she-driving-patent-attorneys-mad-as-hatters/.

[40] Nick Gray, "Apple and HTC Settle All Patent Disputes with 10 Year Cross-Licensing Agreement," *Android and Me* (blog), November 11, 2012, http://androidandme.com/2012/11/news/apple-and-htc-settle-all-patent-disputes-with-10-year-cross-licensing-agreement/?utm_source=feedburnerutm_medium=feedutm_campaign=Feed%3A+androidandme+%28Android+and+Me%29utm_content=NewsGator+Online.

[41] Darryl K. Taft, "IBM Inks Patent Cross-License Deal with Western Digital," *eWeek*, January 25, 2016, www.eweek.com/it-management/ibm-inks-patent-cross-license-deal-with-western-digital.html.

[42] Jim Kerstetter, "How Much Is that Patent Lawsuit Going to Cost You?" c/net, April 5, 2012, https://www.cnet.com/news/how-much-is-that-patent-lawsuit-going-to-cost-you/.

[43] Robert B. Milligan, "U.S. Senate Passes Bill Creating a Civil Cause of Action in Federal Court for Trade Secret Misappropriation," *Trade Secrets Law*, April 5, 2016, www.tradesecretslaw.com/2016/04/articles/trade-secrets/new-year-new-progress-2016-update-on-defend-trade-secrets-act-eu-directive/.

[44] "Uniform Trade Secrets Act," National Conference of Commissioners on Uniform State Laws, http://euro.ecom.cmu.edu/program/law/08-732/TradeSecrets/utsa.pdf (accessed January 15, 2017).

[45] Gerald J. Mossinghoff, J. Derek Mason, and David A. Oblon, "The Economic Espionage Act: A New Federal Regime of Trade Secret Protection," *Oblon Spivak*, www.oblon.com/publications/economic-espionage-act-new-federal-regime-trade-secret-protection.

[46] "Commission on the Theft of American Intellectual Property (The IP Commission) Report, May 2013," *Council on Foreign Relations*, May 22, 2013, www.cfr.org/intellectual-property/commission-theft-american-intellectual-property-ip-commission-report-may-2013/p30925.

[47] Chris Dolmetsch, "Aleynikov on the Hook Again for Taking HFT Code from Goldman," *Bloomberg*, January 24, 2017, https://www.bloomberg.com/news/articles/2017-01-24/aleynikov-s-conviction-is-reinstated-by-state-appeals-court.

[48] Eric E. Bensen, "Defending Trade Secrets under the Economic Espionage Act," *Lexis Practice Advisor Journal* (blog), September 13, 2016, https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2016/09/13/defending-trade-secrets-under-the-economic-espionage-act.aspx.

[49] Matt Schelp, Matt Diehr, and Mark Milton, "Husch Blackwell Files One of First Lawsuits Brought under the Defend Trade Secrets Act of 2016 (DTSA)," *Husch Blackwell*, June 20, 2016, www.tmtindustryinsider.com/2016/06/husch-blackwell-files-one-of-first-lawsuits-brought-under-the-defend-trade-secrets-act-of-2016-dtsa/.

[50] Thomas Claburn, “Apple’s Controversial iPhone Developer Agreement Published,” *InformationWeek*, October 28, 2008, http://www.informationweek.com/mobile/mobile-devices/apples-controversial-iphone-developer-agreement-published-/d/d-id/1073394.

[51] Bill Nolan, “Noncompete Agreements: Critical IP and Employment Protection.” *Columbus CEO*, June 11, 2013, http://www.columbusceo.com/content/stories/2011/01/noncompete-agreements-critical-ip-and-employment-protection.html.

[52] Kevin Simpson, “Rise in Student Plagiarism Cases Attributed to Blurred Lines of Digital World,” *Denver Post*, February 7, 2012, www.denverpost.com/news/ci_19907573.

[53] Jeffrey R. Young, “Dozens of Plagiarism Incidents Are Reported in Coursea’s Free Online Courses,” *Chronicle of Higher Education*, August 16, 2012, chronicle.com/article/Dozens-of-Plagiarism-Incidents/133697.

[54] “About Turnitin,” *Turnitin*, http://turnitin.com/en_us/about-us/our-company (accessed January 16, 2017).

[55] “About iThenticate,” *iThenticate*, www.ithenticate.com/about (accessed January 16, 2017).

[56] “Fourth Circuit Affirms Fair Use Finding Regarding Anti Plagiarism Software,” *Satterlee Stevens Burke and Burke, LLP*, www.ssbb.com/index.php/publications/entry/211 (accessed January 16, 2017).

[57] Joe Wilcox, “There’s Nothing Unusual about Microsoft Reverse Engineering Google Search Results to Improve Bing, But Is It Right?” *betanews*, February 2, 2011, http://betanews.com/2011/02/02/there-s-nothing-unusual-about-microsoft-reverse-engineering-google-search-results-to-improve-bing-but-is-it-right.

[58] “Discover the World of Open Source with Google Code-in 2012,” Google, November 20, 2012, http://googleblog.blogspot.in/2012/11/discover-world-of-open-source-with.html.

[59] “Overview of Trademark Law,” Berkman Klein Center for Internet & Society at Harvard University, https://cyber.harvard.edu/metaschool/fisher/domain/tm.htm (accessed February 12, 2017).

[60] *Playboy Enterprises, Inc. v. Terri Welles*, E-Law Web Page, www.loundy.com/CASES/Playboy_v_Wells.html (accessed January 15, 2017).

[61] Lance Whitney, “Apple Wins Right to Use iPhone Name in Brazil,” *CNET*, September 15, 2013, https://www.cnet.com/news/apple-wins-right-to-use-iphone-name-in-brazil/.

[62] Matt Novak, “5 Domain Name Battles of the Early Web,” *Gizmodo*, November 21, 2014, http://paleofuture.gizmodo.com/5-domain-name-battles-of-the-early-web-1660616980 (accessed February 16, 2017).

CHAPTER 7

ETHICAL DECISIONS IN SOFTWARE DEVELOPMENT

QUOTE

Computers are magnificent tools for the realization of our dreams, but no machine can replace the human spark of spirit, compassion, love, and understanding.
—Louis V. Gerstner, Jr., former CEO and chairman of the board of IBM

Rawpixel.com/Shutterstock.com

ORGANIZATIONS BEHAVING BADLY

Airlines use a variety of information systems to support daily operations such as flight dispatching, flight-path planning (which must take into account multiple factors, including aircraft weight and performance data, en route winds, weather and turbulence forecasts, airspace restrictions, and airport conditions), crew scheduling, passenger check-in, and preflight passenger and baggage weight balancing. Complex software systems also support the airlines' ground-to-cockpit communications, ticket sales, and frequent-flier program administration. As critical as all of these systems are to the daily operations of the airlines, however, the underlying software is often surprisingly buggy and subject to failure. In the six-month time period from August 2016 to February 2017, American, Delta, JetBlue, Southwest Airlines, United Continental, and Virgin America, in total, experienced a dozen system failures, resulting in tens of thousands of flight delays and cancellations, stranded and upset passengers, and hundreds of millions of dollars in lost revenue. These incidents have reinforced the fear among many frequent flyers that such system disruptions are now the norm in the airline industry.

Airlines are typically reluctant to provide details about these operational problems or to communicate the root causes—other than to issue a statement when such a system breakdown occurs, indicating there had been some sort of software failure. However, the frequency and seriousness of these meltdowns demonstrate the vulnerability of the airline computer systems and raise some fundamental underlying questions:

- Over the course of a decade or more, the trend in the U.S. airline industry has been toward consolidation. Large-scale mergers of U.S. airlines—including the mergers of Delta and Northwest (2008–2010), United and Continental (2010–2012), Southwest Airlines and AirTran (2011), and American Airlines and US Airways (2013–2015)—have resulted in an industry in which four large carriers now handle 85 percent of domestic capacity. Have these companies become too large, too complex, and too reliant on information systems?[1]
- Many airline systems are decades old—dating back to the 1990s, or in some cases, even earlier.[2] Although these systems have been updated, patched, and modified to keep up with the many changes in the way the airlines conduct their business, many of them have become increasingly unstable and unreliable. Is it time to discard these legacy systems and build new, more reliable systems from scratch?

- The airlines have implemented a complex infrastructure of interconnected hardware and software. If a glitch occurs in one component of the system, the problem often propagates in a domino effect that can wipe out multiple, important facets of system functionality. Can anything be done to reduce this interdependency of the components of these critical information system?[3]

What decisions have airline management made over the decades that have led to this situation? What measures can the airlines take to improve the situation, and can the cost of these measures be business justified?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What is meant by software quality, why is it so important, and what potential ethical issues do software manufacturers face when making decisions that involve trade-offs between project schedules, project costs, and software quality?
2. What are some effective strategies for developing quality systems?

SOFTWARE QUALITY AND WHY IT IS IMPORTANT

High-quality software systems are systems that are easy to learn and use because they perform quickly and efficiently, they meet their users' needs, and they operate safely and reliably so that system downtime is kept to a minimum. Such software has long been required to support the fields of air traffic control, nuclear power, automobile safety, health care, military and defense, and space exploration. Computers and software are integral parts of almost every business, and the demand for high-quality software in a variety of industries is increasing. End users cannot afford system crashes, lost work, or lower productivity. Nor can they tolerate security holes through which intruders can spread viruses, steal data, or shut down websites. Software manufacturers face economic, ethical, and organizational challenges associated with improving the quality of their software. This chapter covers many of these issues.

A **software defect** is any error that, if not removed, could cause a software system to fail to meet its users' needs. The impact of these defects can be trivial; for example, a computerized sensor in a refrigerator's ice cube maker might fail to recognize that the tray is full and, therefore, continue to make ice. Other defects could lead to tragedy—the control system for an automobile's antilock brakes could malfunction and send the car into an uncontrollable spin. The defect might be subtle and undetectable, such as a tax preparation package that makes a minor miscalculation; or the defect might be glaringly obvious, such as a payroll program that generates checks with no deductions for Social Security or other taxes. Here are some recent, notable software bugs:

- The Nest thermostat is a clever device that enables users to monitor and adjust their thermostats using their smartphones. However, during a recent cold spell, a software glitch caused the devices to shut down or go offline for many customers. Temperatures in their homes plunged over night, threatening to freeze pipes and causing potentially serious health issues for the elderly and ill and those with infants.[4]
- In 2016, software problems resulted in thousands of Blue Cross and Blue Shield of North Carolina customers being overbilled, enrolled in the wrong plans, dropped from coverage, or left without proper insurance cards. In addition, nearly 100 health care providers were unable to properly bill the insurance company for their services—and thus went unpaid—for months.[5]
- A faulty software update at the U.S. Customs and Border Protection agency caused a shutdown of the agency's systems that are used to process travelers. The resulting massive lines and delays at airports ruined the end of vacations for many holiday travelers returning to the United States.[6]
- Functional magnetic resonance imaging (fMRI) is used to create images that are intended to show how various areas of our brains react when we are in REM sleep, playing a game of chess, or exercising strenuously, for example. These pictures have served as the basis of tens of thousands of scientific papers and books. However, flaws in the software used to analyze fMRI data were recently uncovered by scientists who studied the results of many different brain studies over the last 15 years. According to the new report, the software flaw frequently caused false positives, suggesting brain activity where there was none. This has raised considerable controversy between critics who have long said fMRI is nothing more than high-tech pseudo medicine and brain-imaging researchers who claim that the software problems are not as serious or widespread as reported.[7]

Software quality is the degree to which a software product meets the needs of its users. **Quality management** focuses on defining, measuring, and refining the quality of the development process and the products developed during its various stages. These products—including statements of requirements, flowcharts, and user documentation—are known as a **deliverable**. The objective of quality management is to help developers deliver high-quality systems that meet the needs of their users. Unfortunately, the first release of any software rarely meets all its users' expectations. A software product does not usually work as well as its users would like it to until it has been used for a while, found lacking in some ways, and then corrected or upgraded.

One cause of poor software quality is that many developers do not know how to design quality into software from the very start; others simply do not take the time to do so. To develop high-quality software, developers must define and follow a set of rigorous software engineering principles and be committed to learning from past mistakes. In addition, they must understand the environment in which their systems will operate and design systems that are as immune to human error as possible.

All software designers and programmers make mistakes in defining user requirements and turning them into lines of code. Coverity (a software testing firm) performed a sophisticated scan of 17.5 million lines of code from the widely used open source packages Linux, Apache HTTP, MySQL, and Perl/PHP/Python, which are used to run millions of web servers around the world. The study found just 0.290 defects per thousand lines of code.[8] A separate analysis found that about 10 to 20 defects per thousand lines of code are identified during in-house testing of Microsoft's applications. By the time those applications are released to the public, that error rate is in the range of 0.5 defects per thousand lines of code.[9] That means the Microsoft Windows 10 operating system (which contains an estimated 50 million lines of code) may have included close to 25,000 defects at the time it was released. Thus, critical software used daily by workers worldwide likely contains tens of thousands of defects.

Another factor that can contribute to poor-quality software is the extreme pressure that software companies feel to reduce the time to market their products. They are driven by the need to beat the competition in delivering new functionality to users, begin generating revenue to recover the cost of development, and show a profit for shareholders. They are also driven by the need to meet quarterly earnings forecasts used by financial analysts to place a value on the stock. The resources and time needed to ensure quality are often cut under the intense pressure to ship a new product. When forced to choose between adding more user features and doing more testing, most software companies decide in favor of more features. They often reason that defects can be patched in the next release, which will give customers an automatic incentive to upgrade. Additional features make a release more useful and therefore easier to sell to customers.

A major ethical dilemma for software development organizations is: "How much additional cost and effort should we expend to ensure that our products and services meet customers' expectations?" A study published in *the International Journal of Software Engineering & Applications* concluded that approximately 22 percent of Android apps on the market at the time of the study were of low quality. An app was considered to be low quality if it had one or more of the following characteristics that the developer failed to correct over time: included a poor user interface, did not meet the user requirements, had security issues, failed at certain critical moments, had compatibility and downloading issues, consumed excess battery power, or was overly expensive.[10] Customers are stakeholders who are key to the success of a software application, and they may benefit from new features. However, they also bear the burden of errors that aren't caught or fixed during testing.

As a result of the lack of consistent quality in software, many organizations avoid buying the first release of a major software product or prohibit its use in critical systems; their rationale is that the first release often has many defects that cause problems for users. Because of the defects in the first two popular Microsoft operating systems (DOS and Windows), including their tendency to crash unexpectedly, many believe that Microsoft did not have a reasonably reliable operating system until its third major variation—Windows NT.

Even software products that have been reliable over a long period can falter unexpectedly when they are replaced with a newer version. British Airways implemented a new global check-in system in 2016, which led to five major computer outages between May and September. The result was thousands of flights canceled or delayed, tens of thousands of passengers upset and inconvenienced, and a cumulative stock market loss of 10.54 percent or £92.9 billion (USD $113 billion).[11]

The Importance of Software Quality

A **business information system** is a set of interrelated components—including hardware, software, databases, networks, people, and procedures—that collects and processes data and disseminates the output. A common type of business system is one that captures and records business transactions. For example, a manufacturer's order-processing system captures order information, processes it to update inventory and accounts receivable, and ensures that the order is filled and shipped on time to the customer. Other examples are an airline's online ticket reservation system and an electronic funds transfer system that moves money among banks. The accurate, thorough, and timely processing of business transactions is a key requirement for such systems. A software defect can be devastating, resulting in lost customers and reduced revenue. How many times would bank customers tolerate having their funds transferred to the wrong account before they stopped doing business with that bank?

Another type of business information system is the **decision support system (DSS)**, which is used to improve decision making in a variety of industries. A DSS can be used to develop accurate forecasts of customer demand, recommend stocks and bonds for an investment portfolio, or schedule shift workers in such a way as to minimize cost while meeting customer service goals. A software defect in a DSS can result in significant negative consequences for an organization and its customers.

Software is also used to control many industrial processes in an effort to reduce costs, eliminate human error, improve quality, and shorten the time it takes to manufacture products. For example, steel manufacturers use process-control software to capture data from sensors about the equipment that rolls steel into bars and about the furnace that heats the steel before it is rolled. Without process-control computers, workers could react to defects only after the fact and would have to guess at the adjustments needed to correct the process. Process-control computers enable the process to be monitored for variations from operating standards (e.g., a low furnace temperature or incorrect levels of iron ore) and to eliminate product defects before they affect product quality. Any defect in this software can lead to decreased product quality, increased waste and costs, or even unsafe operating conditions for employees.

Software is also used to control the operation of many industrial and consumer products, such as automobiles, medical diagnostic and treatment equipment, televisions, cameras, home security systems, refrigerators, and washers. A software defect could have relatively minor consequences, such as clothes not drying long enough, or it could cause serious damage, such as a patient being overexposed to powerful X-rays.

As a result of the increasing use of computers and software in business, many companies are now in the software business whether they like it or not. The quality of software, its usability, and its timely development are critical to almost everything businesses do. The speed with which an organization develops quality software can put it ahead of or behind its competitors. Mismanaged software can be fatal to a business, causing it to miss product delivery dates, incur increased product development costs, and deliver products that have poor quality.

Business executives frequently face ethical questions of how much money and effort they should invest to ensure the development of high-quality software. A manager who takes a short-term, profit-oriented view may feel that any additional time and money spent on quality assurance will only delay a new product's release, resulting in a delay in sales revenue and profits. However, a different manager may consider it unethical not to fix all known problems before putting a product on the market and charging customers for it.

Other key questions for executives are whether their products could cause damage and what their legal exposure would be if they did. Fortunately, software defects are rarely lethal, and few personal injuries are related to software failures. However, the increasing use of software to control critical functions in vehicles as well as manage the operation of medical devices introduces product liability issues that concern many executives.

Software Product Liability

The liability of manufacturers, sellers, lessors, and others for injuries caused by defective products is commonly referred to as **product liability**. There is no federal product liability law; instead, product liability in the United States is mainly covered by common law (made by state judges) and Article 2 of the Uniform Commercial Code, which deals with the sale of goods.

If a software defect causes injury or loss to purchasers, lessees, or users of the product, the injured parties may be able to sue as a result. Injury or loss can come in the form of physical mishaps and death, loss of revenue, or an increase in expenses due to a business disruption caused by a software failure. Numerous product liability claims may well be in the future for the self-driving car based upon product liability claims against the vehicle manufacturer or a supplier of a component. This would come about if there was a malfunction in the electronics or software of the vehicle that lead to injuries or property damage.

Software product liability claims are typically based on strict liability, negligence, breach of warranty, or misrepresentation—sometimes in combination with one another. Each of these legal concepts is discussed in the following paragraphs.

Strict liability means that the defendant is held responsible for injuring another person, regardless of negligence or intent. The plaintiff must prove only that the software product is defective or unreasonably dangerous and that the defect caused the injury. There is no requirement to prove that the manufacturer was careless or negligent, or to prove who caused the defect. All parties in the chain of distribution—the manufacturer, subcontractors, and distributors—are strictly liable for injuries caused by the product and may be sued.

Defendants in a strict liability action may use several legal defenses, including the doctrine of supervening event, the government contractor defense, and an expired statute of limitations. Under the doctrine of supervening event, the original seller is not liable if the software was materially altered after it left the seller's possession and the alteration caused the injury. To establish the government contractor defense, a contractor must prove that the precise software specifications were provided by the government, that the software conformed to the specifications, and that the contractor warned the government of any known defects in the software. Finally, there are statutes of limitations for claims of liability, which means that an injured party must file suit within a certain amount of time after the injury occurs.

Negligence is the failure to do what a reasonable person would do, or doing something that a reasonable person would not do. When sued for negligence, a software supplier is not held responsible for every product defect that causes customer or third-party loss. Instead, responsibility is limited to harmful defects that could have been detected and corrected through "reasonable" software development practices. Contracts written expressly to limit claims of supplier negligence may be disregarded by the courts as unreasonable. Software manufacturers and organizations with software-intensive products are frequently sued for negligence and must be prepared to defend themselves.

The defendant in a negligence case may either answer the charge with a legal justification for the alleged misconduct or demonstrate that the plaintiffs' own actions contributed to their injuries (**contributory negligence**). If proved, the defense of contributory negligence can reduce or totally eliminate the amount of damages the plaintiffs receive. For example, if a person uses a pair of pruning shears to trim his fingernails and ends up cutting off a fingertip, the defendant could claim contributory negligence.

A **warranty** assures buyers or lessees that a product meets certain standards of quality. A warranty of quality may be either expressly stated or implied by law. Express warranties can be oral, written, or inferred from the seller's conduct. For example, sales contracts contain an implied warranty of merchantability, which requires that the following standards be met:

- The goods must be fit for the ordinary purpose for which they are used.
- The goods must be adequately contained, packaged, and labeled.
- The goods must be of an even kind, quality, and quantity within each unit.
- The goods must conform to any promise or affirmation of fact made on the container or label.
- The quality of the goods must pass without objection in the trade.
- The goods must meet a fair average or middle range of quality.

If the product fails to meet the terms of its warranty, the buyer or lessee can sue for **breach of warranty**. Of course, most dissatisfied customers will first seek a replacement, a substitute product, or a refund before filing a lawsuit.

Software suppliers frequently write warranties to attempt to limit their liability in the event of nonperformance. Although a certain software application may be warranted to run on a given machine configuration, often no assurance is given as to what that software will do. However, even if a contract specifically excludes the commitment of merchantability and fitness for a specific use, the court may find such a disclaimer clause unreasonable and refuse to enforce it or refuse to enforce the entire contract. In determining whether warranty disclaimers are unreasonable, the court attempts to evaluate if the contract was made between two "equals" or between an expert and a novice. The relative education, experience, and bargaining power of the parties and whether the sales contract was offered on a take-it-or-leave-it basis are considered in making this determination.

The plaintiff must have a valid contract that was unfulfilled by the supplier in order to win a breach-of-warranty claim. Because the software supplier writes the warranty, this claim can be extremely difficult to prove. For example, the M. A. Mortenson Company—one of the largest construction companies in the United States—installed a new version of bid-preparation software for use by its estimators. During the course of preparing one bid, the software allegedly malfunctioned several times, each time displaying the same cryptic error message. Nevertheless, the estimator submitted the bid and Mortenson won the contract.

Afterward, Mortenson discovered that the bid was $1.95 million lower than intended, and the company filed a breach-of-warranty suit against Timberline Software, makers of the bid software. Timberline acknowledged the existence of the bug. However, the courts ruled in Timberline's favor because the license agreement that came with the software explicitly barred recovery of the losses claimed by Mortenson.[12] Even if breach of warranty can be proven, damages are generally limited to the amount of money paid for the product.

Intentional misrepresentation occurs when a seller or lessor either misrepresents the quality of a product or conceals a defect in it. For example, if a cleaning product is advertised as safe to use in confined areas and some users subsequently pass out from the product's fumes, they could sue the seller for intentional misrepresentation or fraud. Advertising, salespersons' comments, invoices, and shipping labels are all forms of representation. Most software manufacturers use limited warranties and disclaimers to avoid any claim of misrepresentation.

CRITICAL THINKING EXERCISE: SOFTWARE WARRANTY

You are a member of the legal department of a relatively new software firm, which is about to release its first product after two years of development. The software was developed for use by owners of rental property and is capable of doing all the necessary accounting, including the calculation of state and federal income taxes, associated with the property rental business. The software has an impressive array of features—many more, in fact, than its competitors—and is priced very competitively.

You have been struggling to define the terms of the warranty that will accompany the software product. You want to keep the warranty simple to limit the firm's potential liability in the event it does not meet the expectations of customers. The head of software development, on the other hand, wants to create a warranty that will stand out as far superior to the competition in that it spells out the specifics of what the software will and will not do. What are the pros and cons of each approach?

STRATEGIES FOR DEVELOPING QUALITY SOFTWARE

As individuals and organizations have come to increasing rely on software, developers have identified multiple strategies for ensuring the quality of their software. These include the use of tools such as software development methodologies, the Capability Maturity Model Integration (CMMI) process-improvement model, special techniques for safety-critical systems, risk management processes, and quality management standards. These topics will be discussed in the following sections.

Software Development Methodologies

Developing information system software is not a simple process; it requires completing many complex activities, with many dependencies among the various activities. System analysts, programmers, hardware engineers, infrastructure architects, database specialists, project managers, documentation specialists, trainers, and testers are all involved in large software projects. Each of these groups of workers has a role to play, with specific responsibilities and tasks. In addition, each group makes decisions that can affect the software's quality and the ability of an organization or an individual to use it effectively.

Most software companies have adopted a specific **software development methodology**—a standard, proven work process that enables systems analysts, programmers, project managers, and others to make controlled and orderly progress in developing high-quality software. A methodology defines activities in the software development process as well as the individual and group responsibilities for accomplishing these activities (see Figure 7-1). Each methodology recommends specific techniques for accomplishing the various activities, such as using a flowchart to document the logic of a computer program. A methodology also offers guidelines for managing the quality of software during the various stages of development. If an organization has developed such a methodology, it is typically applied to any software development that the company undertakes.

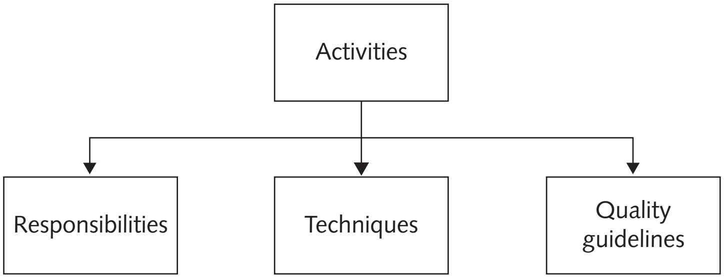


FIGURE 7-1 Components of a software development methodology

The **waterfall system development model** is a sequential, multistage system development process in which development of the next stage of the system cannot begin until the results of the current stage are approved or modified as necessary. This approach is referred to as a waterfall process because progress is seen as flowing steadily downward (like a waterfall) through the various stages of the development. The stages of development can vary from one organization to the next, with many organizations using an approach with six stages as shown in Figure 7-2.

Under the **agile development** methodology, a system is developed in iterations (often called sprints) lasting from one to four weeks, as illustrated in Figure 7-3. Unlike the waterfall system development model, agile development accepts the fact that system requirements are evolving and cannot be fully understood or defined at the start of the project. Agile development concentrates instead on maximizing the team's ability to deliver quickly and respond to emerging requirements—hence the name agile. In an agile development project, the team evaluates the system every one to four weeks, giving it ample opportunity to identify and implement new requirements. The Manifesto for Agile Software Development (https://www.agilealliance.org/agile101/the-agile-manifesto) was developed by a group of software practitioners. The manifesto is built around a set of 4 values and 12 principles that help agile project teams make ethical decisions in the development of quality software.

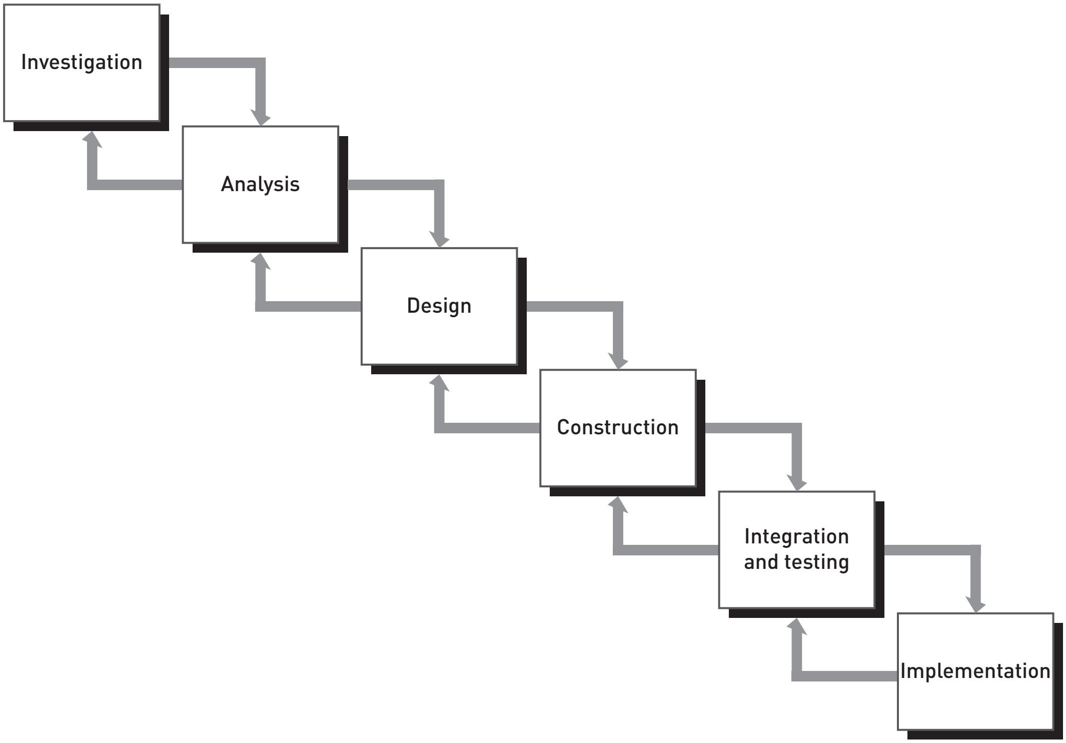


FIGURE 7-2 Waterfall system development model

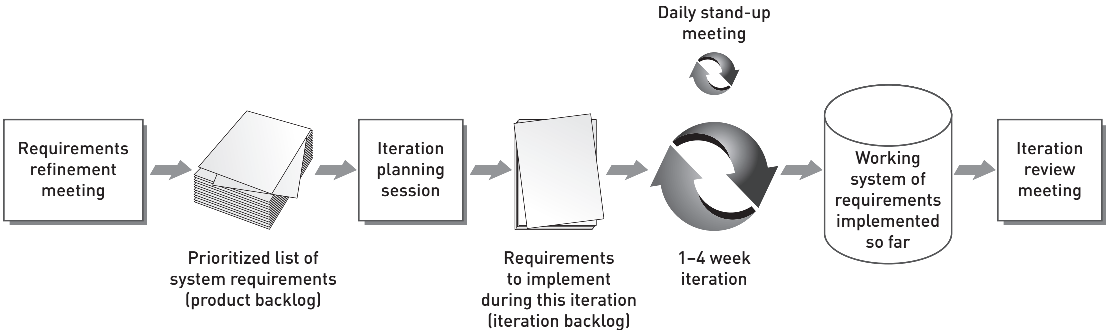

Daily stand-up meeting
Requirements refinement meeting
Prioritized list of system requirements (product backlog)
Iteration planning session
Requirements to implement during this iteration (iteration backlog)
1–4 week iteration
Working system of requirements implemented so far
Iteration review meeting

FIGURE 7-3 Agile system development methodology

Table 7-1 summarizes the pros and cons of these two approaches to system development.

TABLE 7-1 Pros and cons of waterfall and agile

Waterfall		Agile	
Pros	**Cons**	**Pros**	**Cons**
Formal review at end of each stage allows maximum management control.	Often, users' needs go unstated or are miscommunicated or misunderstood. Users may end up with a system that meets those needs as understood by the developers; however, this might not be what the users really needed.	For appropriate projects, this approach puts an application into production sooner.	It is an intense process that takes considerable time and effort on the part of project members and can result in burnout for system developers and other project participants.
Structured processes produce many intermediate products that can be used to measure progress toward developing the system.	Users can't easily review intermediate products and evaluate whether a particular product will lead to a system that meets their business requirements.	Forces teamwork and lots of interaction between users and project stakeholders so that users are more likely to get a system that meets their needs.	Requires stakeholders and users to spend more time working together on the project.

As with most things, it is usually easier and cheaper to avoid software problems at the beginning than to attempt to fix the damages after the fact. Studies have shown that the cost to identify and remove a defect in an early stage of software development can be up to 100 times less than removing a defect in a piece of software that has been distributed to customers (see Figure 7-4).[13,14] (Although these studies were conducted several years ago, their results still hold true today.)

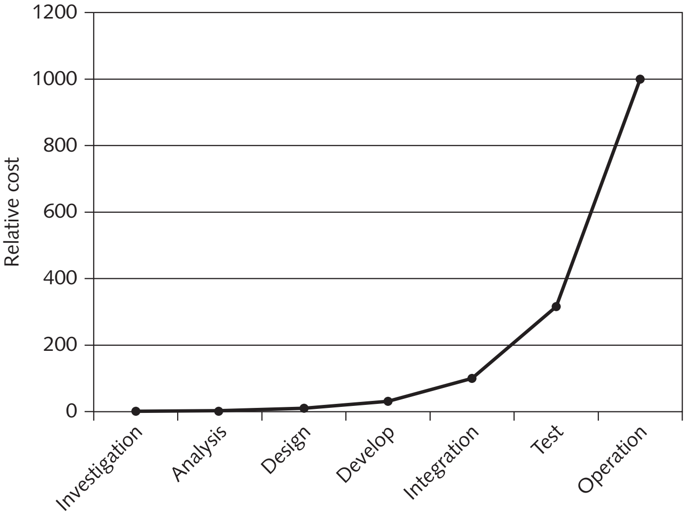


FIGURE 7-4 The cost of removing defects

Source: Used with permission from LKP Consulting Group.

If a defect is uncovered during a later stage of development, some rework of the deliverables produced in preceding stages will be necessary. The later the error is detected, the greater the number of people who will be affected by the error; thus, the greater the costs will be to communicate and fix the error. Consider the cost to communicate the details of a defect, distribute and apply software fixes, and possibly retrain end users for a software product that has been sold to hundreds or thousands of customers. Thus, most software developers try to identify and remove errors early in the development process not only as a cost-saving measure but also as the most efficient way to improve software quality.

A product containing inherent defects that harm the user may be the subject of a product liability suit. The use of an effective methodology can protect software manufacturers from legal liability in two ways. First, an effective methodology reduces the number of software errors that might occur. Second, if an organization follows widely accepted development methods, negligence on its part is harder to prove. However, even a successful defense against a product liability case can cost hundreds of thousands of dollars in legal fees. Thus, failure to develop software carefully and consistently can have serious consequences in terms of liability exposure.

Quality assurance (QA) refers to methods within the development process that are designed to guarantee reliable operation of a product. Ideally, these methods are applied at each stage of the development cycle. However, some software manufacturing organizations without a formal, standard approach to QA consider testing to be their only QA method. Instead of checking for errors throughout the development process, such companies rely primarily on testing just before the product is shipped to ensure some degree of quality.

Several types of tests are used in software development, as discussed in the following section.

Software Testing

Software is developed in units called subroutines or programs. These units, in turn, are combined to form large systems. One approach to QA is to test the code for a completed unit of software by actually entering test data and comparing the results to the expected results in a process called **dynamic testing**. There are two forms of dynamic testing:

- **Black-box testing** involves viewing the software unit as a device that has expected input and output behaviors but whose internal workings are unknown (a black box). If the unit demonstrates the expected behaviors for all the input data in the test suite, it passes the test. Black-box testing takes place without the tester having any knowledge of the structure or nature of the actual code. For this reason, it is often done by someone other than the person who wrote the code.
- **White-box testing** treats the software unit as a device that has expected input and output behaviors but whose internal workings, unlike the unit in black-box testing, are known. White-box testing involves testing all possible logic paths through the software unit with thorough knowledge of its logic. The test data must be carefully constructed so that each program statement executes

at least once. For example, if a developer creates a program to calculate an employee's gross pay, the tester would develop data to test cases in which the employee worked less than 40 hours, exactly 40 hours, and more than 40 hours (to check the calculation of overtime pay).

Other forms of software testing include the following:

- **Static testing**—This is a software-testing technique in which software is tested without actually executing the code. It consists of two steps—review and static analysis. During the review step, analysts and/or programmers review pertinent documentation to find and eliminate any errors in system requirements or design specifications. They also read the code that has been written. There are several types of review—informal, walk-through, peer review, and inspection—in increasing order of effort and thoroughness. During the static analysis step, special software programs called static analyzers are run against the code. Rather than reviewing input and output, the static analyzer looks for suspicious patterns in programs that might indicate a defect. Static analyzers can identify the following types of errors: a variable with an undefined value, variables that are declared but never used, unreachable code that can never be executed, programming standards violations, and potential system security vulnerabilities. Static testing can be performed while the code is being written, prior to any other type of testing, which gives static testing an important advantage in that it can detect and eliminate defects early in the software development process when they are easier and less costly to fix.
- **Unit testing**—This involves testing individual components of code (subroutines, modules, and programs) to verify that each unit performs as intended. Unit testing is accomplished by developing test data that ideally force the code to execute all of its various functions and user features. As testers find problems, they modify the code to work correctly.
- **Integration testing**—After successful unit testing, the software units are combined into an integrated subsystem that undergoes rigorous testing to ensure that the linkages among the various subsystems work successfully.
- **System testing**—After successful integration testing, the various subsystems are combined to test the entire system as a complete entity.
- **User acceptance testing**—Trained end users conduct independent user acceptance testing to ensure that the system operates as they expect.

Capability Maturity Model Integration

Capability Maturity Model Integration (CMMI) models are collections of best practices that help organizations improve their processes. A **best practice** is a method or technique that has consistently shown results superior to those achieved with other means, and that is used as a benchmark within a particular industry. CMMI models are developed by product teams with members from industry, government, and the Carnegie Mellon Software Engineering Institute (SEI). The models are general enough to be used to evaluate and improve almost any process, and a specific application of CMMI—**CMMI-Development (CMMI-DEV)**—is frequently used to assess and improve software development practices. There are additional CMMI applications for the acquisition and delivery of products and services. CMMI defines five levels of software development maturity (see Table 7-2) and identifies the issues that are most critical to software quality and process improvement. A maturity level consists of practices for a set of process areas that improve an organization's overall performance. Identifying an organization's current maturity level enables it to specify necessary actions to improve the organization's future performance. The model also enables an organization to track, evaluate, and demonstrate its progress over the years. From 2007 to June 2016, more than 13,700 CMMI appraisals of organizations have been performed. Of these, only 11 percent were determined to be high-maturity (level 4 or 5) organizations.[15]

TABLE 7-2 Definition of CMMI maturity levels

Maturity level	Description
Initial	Process is ad hoc and chaotic; organization tends to overcommit and processes are often abandoned during times of crisis.
Managed	Projects employ processes and skilled people; status of work products is visible to management at defined points.
Defined	Processes are well defined and understood and are described in standards, procedures, tools, and methods; processes are consistent across the organization.
Quantitatively managed	Quantitative objectives for quality and process performance are established and are used as criteria in managing projects; specific measures of process performance are collected and statistically analyzed.
Optimizing	Organization continually improves its processes; changes are based on a quantitative understanding of its business objectives and performance needs.

Source: Used with permission from Carnegie Mellon University.

CMMI-DEV is a set of guidelines for 22 process areas related specifically to systems development. The premise of the model is that those organizations that do these 22 things well will have an outstanding software development process. After an organization decides to adopt CMMI-DEV, it must conduct an assessment of its software development practices (using trained, outside assessors to ensure objectivity) to determine where the organization fits in the capability model. The assessment identifies areas for improvement and establishes action plans needed to upgrade the development process. Over the course of a few years, the organization can improve its maturity level by executing the action plan.

CMMI-DEV can also be used as a benchmark for comparing organizations. In the awarding of software contracts—particularly by the federal government—organizations that bid on a contract may be required to have adopted CMMI and to be performing at a certain level.

Achieving Maturity Level 5—the highest possible rating—is a significant accomplishment for any organization, and it can lead to substantial business benefits. It means that the organization is able to statistically evaluate the performance of its software development processes. This in turn leads to better control and continual improvement in the processes, making it possible to deliver software products of high quality on time and on budget.

Honeywell is a Fortune 100 company that provides aerospace products and services, control technologies for homes and businesses, turbochargers, and performance materials to customers around the world. Quality software development is a critical part of Honeywell's commitment to produce high-quality, software-enabled products. The company has achieved CMMI Maturity Level 5 in 100 percent of its global software divisions, enabling its software teams to develop better products, faster and at a lower cost—providing Honeywell with an important competitive advantage. According to Honeywell chairman and CEO Dave Cote, "Like total quality management, a best practice widely adopted in Western manufacturing companies, CMMI is a similar best practice in software engineering."[16]

Developing Safety-Critical Systems

Although defects in any system can cause serious problems, the consequences of software defects in certain systems can be deadly. In these kinds of systems, the stakes involved in creating quality software are raised to the highest possible level. The ethical decisions involving a trade-off—if one must be considered—between quality and factors such as cost, ease of use, and time to market require extremely serious examination.

A **safety-critical system** is one whose failure may cause human injury or death. The safe operation of many safety-critical systems relies on the flawless performance of software. Such systems control an ever-increasing array of products and applications, including antilock brakes, adaptive cruise control functionality, and a myriad of other safety-related features found in newer automobiles; nuclear power plant reactors; airplane navigation; elevators; and a wide range of medical devices. The process of building software for such systems requires highly trained professionals, formal and rigorous methods, and state-of-the-art tools. Failure to take strong measures to identify and remove software errors from safety-critical systems "is at best unprofessional and at worst leads to disastrous consequences."[17] However, even with these types of precautions, the software associated with safety-critical systems is still vulnerable to errors that can lead to injury or death. The following are some examples of safety-critical system failures:

- Problems with uncontrollable acceleration and a faulty antilock braking system resulted in lost lives and required Toyota to issue three separate recalls costing it nearly $3 billion.[18]
- Neonatal ventilators manufactured by Covidien were recalled because a software problem caused the amount of air being delivered to the patient to be less that the amount specified by the physician or nurse. The problem could lead to serious injury or death.[19]
- As many as 4.3 million General Motors cars and trucks were recalled because they had potentially defective airbags that may fail to deploy in an accident due to flawed embedded software in the vehicles.[20]

When developing safety-critical systems, a key assumption must be that safety will *not* automatically result from following an organization's standard development methodology. Safety-critical software must go through a much more rigorous and time-consuming development process than other kinds of software. All tasks—including requirement definition, systems analysis, design, coding, fault analysis, testing, implementation, and change control—require additional steps, more thorough documentation, and vigilant checking and rechecking. As a result, safety-critical software takes much longer to complete and is much more expensive to develop.

Software developers working on a safety-critical system must also recognize that the software is only one component of the system; other components typically include system users or operators, hardware, and other equipment. Software developers need to work closely with safety and systems engineers to ensure that the entire system, not just the software, operates in a safe manner.

The key to ensuring that these additional tasks are completed is to appoint a **system safety engineer**, who has explicit responsibility for the system's safety. The safety engineer uses a logging and monitoring system to track hazards from a project's start to its finish. This **hazard log** is used at each stage of the software development process to assess how it has accounted for detected hazards. Safety reviews are held throughout the development process, and a robust configuration management system tracks all safety-related matters. However, the safety engineer must keep in mind that his or her role is not simply to produce a hazard log but rather to influence the design of the system to ensure that it operates safely when put into use.

The increased time and expense of completing safety-critical software can draw developers into ethical dilemmas. For example, the use of hardware mechanisms to back up or verify critical software functions can help ensure safe operation and make the consequences of software defects less critical. However, such hardware may make the final product more expensive to manufacture or harder for the user to operate—potentially making the product less attractive than a competitor's. Companies must carefully weigh these issues to develop the safest possible product that also appeals to customers.

Another key issue is deciding when the QA staff has performed sufficient testing. How much testing is enough when you are building a product whose failure could cause loss of human life? At some point, software developers must determine that they have completed sufficient QA activities and then sign off to indicate their approval. Determining how much testing is sufficient demands careful decision making.

In an October 2015 memo, Dr. J. Michael Gilmore, the director of operational test and evaluation for the U.S. Department of Defense, identified 27 category 1 and 64 category 2 deficiencies (many of which are software related) in the advanced F-35 stealth fighter. A category 1 deficiency is defined as a deficiency that "may cause death, severe injury, or severe occupational illness; may cause loss or major damage to a weapon system; critically restrict the combat readiness capabilities of the using organization; or result in a production line stoppage." Category 2 deficiencies "impede or constrain successful mission accomplishment," but are not life-threatening to the pilot or as detrimental to mission success as category 1 deficiencies.[21] The military faces difficult decisions regarding the need to eliminate these deficiencies while still trying to put the aircraft into service at the earliest possible date and hold down project costs.

When designing, building, and operating a safety-critical system, a great deal of effort must be put into considering what can go wrong, the likelihood and consequences of such occurrences, and how risks can be averted, mitigated, or detected so the users can be warned. One approach to answering these questions is to conduct a formal risk analysis.

Risk Management

Risk is the potential of gaining or losing something of value. Risk can be quantified by three elements: a risk event, the probability of the event happening, and the impact (positive or negative) on the business outcome if the risk does actually occur. The **annualized rate of occurrence (ARO)** is an estimate of the probability that this event will occur over the course of a year. The **single loss expectancy (SLE)** is the estimated loss that would be incurred if the event happens. The **annualized loss expectancy (ALE)** is the estimated loss from this risk over the course of a year. The following equation is used to calculate the annual loss expectancy:

$$\text{ARO} \times \text{SLE} = \text{ALE}$$

For example, if an undesirable event has a one percent probability of occurring over the course of a year (ARO) and the consequences of that event occurring would cost $1,000,000 (SLE), then the annualized loss expectancy (ALE) can be calculated as:

$$0.01 \times \$1{,}000{,}000 = \$10{,}000$$

The risk for this event would be considered greater than that of an event that has a 10 percent probability of occurring, at a cost of $50,000 per occurrence.

$$.10 \times \$50{,}000 = \$5{,}000$$

Risk management is the process of identifying, monitoring, and limiting risks to a level that an organization is willing to accept. The level of risk that remains after managing risk is called residual risk. Ultimately, senior management must choose a level of acceptable residual risk based on the organization's goals and the resources (people, dollars, and time) the organization is willing to dedicate to mitigate the risk. Strategies for addressing a particular risk include the following:

- **Acceptance**—When the cost of avoiding a risk outweighs the potential loss of a risk, an organization will likely accept the risk. For example, spending $1 million to avoid a risk that might cost the organization $1,000 per year clearly doesn't make sense. A decision to accept a risk can be extremely difficult and controversial when dealing with safety-critical systems because making that determination involves forming personal judgments about the value of human life, assessing potential liability in case of an accident, evaluating the potential impact on the surrounding natural environment, and estimating the system's costs and benefits.
- **Avoidance**—An organization may choose to eliminate the vulnerability that gives rise to a particular risk in order to avoid the risk altogether. This is the most effective solution, but often not possible due to organizational requirements and factors beyond an organization's control.
- **Mitigation**—Risk mitigation involves the reduction in either the likelihood or the impact of the occurrence of a risk. **N-version programming** is an approach to minimizing the impact of software errors by independently implementing the same set of user requirements *N* times (where *N* could be 2, 3, 4 or more); *N* versions of software are run in parallel; and, if a difference is found, a "voting algorithm" is executed to determine which result to use. For example, if two software versions calculated the answer to a particular

question to be 2.4 and the third version calculated 4.1, the algorithm might choose 2.4 as the correct answer. In N-version programming, each software version is built by different teams of people using different approaches to write programming instructions designed to meet the user's requirements. In some cases, instructions are written by teams of programmers from different companies and run on different hardware devices. The rationale behind N-version programming is that multiple software versions are highly unlikely to fail at the same time under the same conditions. Thus, one or more of versions should yield a correct result. Triple-version programming is common in airplane and spacecraft control systems.

- **Redundancy** is the provision of multiple interchangeable components to perform a single function in order to cope with failures and errors. An example of a simple redundant system would be an automobile with a spare tire or a parachute with a backup chute attached. A more complex redundant system is a redundant array of independent disks (RAID), which is commonly used in high-volume data storage for file servers. RAID systems use many small-capacity disk drives to store large amounts of data to provide increased reliability and redundancy. Should one of the drives fail, it can be removed from service and a new one substituted in its place.
- **Transference**—A common way to accomplish risk transference is for an individual or an organization to purchase insurance, such as auto or business liability insurance. Another way to transfer risk is to outsource the risk by contracting with a third party to manage the risk.

Manufacturers of safety-critical systems must sometimes decide whether to recall a product when data indicate a problem. For example, automobile manufacturers have been known to weigh the cost of potential lawsuits against that of a recall. Drivers and passengers in affected automobiles (and, in many cases, the courts) have not found this approach to be ethically sound. Manufacturers of medical equipment and airplanes have sometimes made similar decisions. Making such a decision is often extremely complicated, especially if the available data cannot pinpoint the cause of a particular problem. For example, there was great controversy over the use of Firestone tires on Ford Explorers after numerous tire blowouts and Explorer rollovers caused multiple injuries and deaths. However, it was difficult to determine if the rollovers were caused by poor automobile design, faulty tires, or improperly inflated tires. Consumers' confidence in both manufacturers and their products was nevertheless shaken.

Reliability is a measure of the rate of failure in a system that would render it unusable over its expected lifetime. For example, if a component has a reliability of 99.9 percent, it has a one in one thousand chance of failing over its lifetime. Although this chance of failure may seem low, remember that most systems are made up of many components. As you add more components, the system becomes more complex, and the chance of failure increases. For example, assume that you are building a complex system made up of seven components, each with 99 percent reliability. If none of the components has redundancy built in, the system has a 93.8 percent ($.99^7$) probability of operating successfully with no component malfunctions over its lifetime. If you build the same type of system using 10 components, each with 99 percent reliability, the overall probability of operating without an individual component failure falls to 90 percent. Thus, building redundancy into systems that are both complex and safety critical is imperative. System engineers sometimes refer to a system with "five nines" (99.999 percent) reliability. This translates to a system that would have only 5.4 minutes of total downtime in a year.

Reliability and safety are two different system characteristics. Reliability has to do with the capability of the system to continue to perform; safety has to do with the ability of the system to perform in a safe manner. Thus, a system could be reliable but not safe. For example, an antiaircraft missile control system may continue to operate under a wide range of operating conditions so that it is considerably reliable. If, however, the control system directs the missile to change direction and to fly back into its launching device, it is certainly unsafe.

One of the most important and challenging areas of safety-critical system design is the system–human interface. Human behavior is not nearly as predictable as the performance of hardware and software components in a complex system. The system designer must consider what human operators might do to make a system work less safely or effectively. The challenge is to design a system that works as it should and leaves little room for erroneous judgment on the part of the operator. For instance, a self-medicating pain-relief system must allow a patient to press a button to receive more pain reliever, but must also regulate itself to prevent an overdose. Additional risk can be introduced if a designer does not anticipate the information an operator needs and how the operator will react under the daily pressures of actual operation, especially in a crisis. Some people keep their wits about them and perform admirably in an emergency, but others may panic and make a bad situation worse.

Poor design of a system interface can greatly increase risk, sometimes with tragic consequences. For example, in July 1988, the guided missile cruiser USS *Vincennes* mistook an Iranian Air commercial flight for an enemy F-14 jet fighter and shot the airliner down over international waters in the Persian Gulf. All 290 people on board were killed. Some investigators blamed the tragedy on a lack of training and experience on the part of the operators and the confusing interface of the $500-million Aegis radar and weapons control system. The Aegis radar on the *Vincennes* locked onto an Airbus 300, but it was misidentified as a much smaller F-14 by its human operators. The Aegis operators also misinterpreted the system signals and thought that the target was descending, even though the airbus was actually climbing. A third human error was made in determining the target altitude—it was off by 4,000 feet. As a result of this combination of human errors, the *Vincennes* crew thought the ship was under attack and shot down the plane.[22]

Quality Management Standards

The International Organization for Standardization (ISO), founded in 1947, is a worldwide federation of national standards bodies from 161 countries. The ISO issued its 9000 series of business management standards in 1988. These standards require organizations to develop formal quality-management systems that focus on identifying and meeting the needs, desires, and expectations of their customers.

The **ISO 9001 family of standards** serves as a guide to quality products, services, and management. ISO 9001 provides a set of standardized requirements for a quality management system. In 2015, more than 1.5 million ISO 9001 certificates were issued to organizations around the world.[23] ISO standards are updated every five years to keep them current and relevant. Although companies can use the ISO standards as a management guide for their own purposes in achieving effective control, the priority for many companies is having a qualified external agency certify that they have achieved ISO 9001 certification. Many businesses and government agencies both in the United States and abroad insist that a potential vendor or business partner have a certified quality management system in place as a condition of doing business. Becoming ISO 9001 certified provides proof of an organization's commitment to quality management and continuous improvement.

To obtain this coveted certificate, an organization must submit to an examination by an external assessor and must fulfill the following requirements:

- Have written procedures for all processes
- Follow those procedures
- Prove to an auditor that it has fulfilled the first two requirements; this proof can require observation of actual work practices and interviews with customers, suppliers, and employees

Many software development organizations are applying for ISO 9001 to meet the special needs and requirements associated with the purchase, development, operation, maintenance, and supply of computer software.

Failure Mode and Effects Analysis

Failure mode and effects analysis (FMEA) is an important technique used to develop ISO 9000–compliant quality systems by both evaluating reliability and determining the effects of system and equipment failures. Failures are classified according to their impact on a project's success, personnel safety, equipment safety, customer satisfaction, and customer safety. The goal of FMEA is to identify potential design and process failures early in a project, when they are relatively easy and inexpensive to correct.

A **failure mode** describes how a product or process could fail to perform the desired functions described by the customer. An effect is an adverse consequence that the customer might experience. Unfortunately, most systems are so complex that there is seldom a one-to-one relationship between cause and effect. Instead, a single cause may have multiple effects, and a combination of causes may lead to one effect or multiple effects. It is not uncommon for a FMEA of a system to identify 50 to 200 potential failure modes.

The use of FMEA helps to prioritize those actions necessary to reduce potential failures with the highest relative risks. The following steps are used to identify the highest priority actions to be taken:

- Determine the severity rating: The potential effects of a failure are scored on a scale of 1 to 10 (or 1 to 5) with 10 assigned to the most serious consequence (9 or 10 are assigned to safety- or regulatory-related effects).
- Determine the occurrence rating: The potential causes of that failure occurring are also scored on a scale of 1 to 10, with 10 assigned to the cause with the greatest probability of occurring.

- Determine the criticality: Criticality is the product of severity times occurrence.
- Determine the detection rating: The ability to detect the failure in advance of it occurring due to the specific cause under consideration is also scored on a scale of 1 to 10, with 10 assigned to the failure with the least likely chance of advance detection. For software, the detection rating would represent the ability of planned tests and inspections to remove the cause of a failure.
- Calculate the risk priority rating: The severity rating is multiplied by the occurrence rating and by the detection rating to arrive at the risk priority rating.

Raytheon is a technology company that designs and manufactures aerospace and defense systems that incorporate cutting-edge electronic components. The company employs 63,000 people worldwide and generated $24 billion in recent sales.[24] Raytheon employs FMEA throughout its product development lifecycle. Starting early in the design cycle, the company invites suppliers to review its designs to identify potential failure modes, assess the ability to detect the modes, and estimate the severity of the effects. Raytheon then uses this input to prioritize the product design issues that need to be eliminate or mitigated to create superior products.[25]

Table 7-3 shows a sample FMEA risk priority table.

TABLE 7-3 Sample FMEA risk priority table

Issue	Severity	Occurrence	Criticality	Detection	Risk priority
#1	3	4	12	9	108
#2	9	4	36	2	72
#3	4	5	20	4	80

Many organizations consider those issues with the highest criticality rating (severity × occurrence) as the highest priority issues to address. They may then go on to address those issues with the highest risk priority (severity × occurrence × detection). So although Issue #2 shown in Table 7-3 has the lowest risk priority, it may be assigned the highest priority because of its high criticality rating.

Table 7-4 provides a manager's checklist for upgrading the quality of the software an organization produces. The preferred answer to each question is *yes*.

TABLE 7-4 Manager's checklist for improving software quality

Question	Yes	No
Has senior management made a commitment to develop quality software?		
Have you used CMMI to evaluate your organization's software development process?		
Has your company adopted a standard software development methodology?		
Does the methodology place a heavy emphasis on quality management and address how to define, measure, and refine the quality of the software development process and its products?		
Are software project managers and team members trained in the use of this methodology?		
Are software project managers and team members held accountable for following this methodology?		
Is a strong effort made to identify and remove errors as early as possible in the software development process?		
Are both static and dynamic software testing methods used?		
Are white-box testing and black-box testing methods used?		
Has an honest assessment been made to determine if the software being developed is safety critical?		
If the software is safety critical, are additional tools and methods employed, and do they include the following: a project safety engineer, hazard logs, safety reviews, formal configuration management systems, rigorous documentation, risk analysis processes, and the FMEA technique?		

CRITICAL THINKING EXERCISE: FAULTY AIRBAG SOFTWARE

You are the software development manager for an organization that produces the software used to control the deployment of airbags used in several popular U.S. automobiles. Last year, vehicles using your software were involved in 200,000 crashes, and 4,000 people died as a result of those accidents. An internal investigation conducted by your firm revealed that at least 40 of those fatalities occurred when airbags failed to deploy properly because of software problems. The cost to develop an improved version of the software is estimated to be in the neighborhood of $10 to $20 million. Simulations have shown that proper deployment of the airbags would likely have reduced the number of fatalities from over 40 to less than 10. Should your firm make the investment necessary to upgrade the software and install it in all new vehicles?

The Department of Transportation's National Highway Traffic Safety Administration (NHTSA) has the authority to issue vehicle safety standards and to require manufacturers to recall vehicles that have safety-related defects. If your firm chooses to inform the NHTSA of its findings and a recall is issued, it will cost an additional $250 million to execute the recall and upgrade existing airbags to the new software. Should your firm work with NHTSA to execute a recall and install the new software in all vehicles—old and new?

Summary

What is meant by software quality, why is it so important, and what potential ethical issues do software manufacturers face when making decisions that involve trade-offs between project schedules, project costs, and software quality?

- High-quality software systems are easy to learn and use. They perform quickly and efficiently to meet their users' needs, operate safely and reliably, and have a high degree of availability that keeps unexpected downtime to a minimum.
- High-quality software has long been required to support the fields of air traffic control, nuclear power, automobile safety, health care, military and defense, and space exploration.
- Computers and software are integral parts of almost every business, and the demand for high-quality software is increasing. End users cannot afford system crashes, lost work, or lower productivity. Nor can they tolerate security holes through which intruders can spread viruses, steal data, or shut down websites.
- A software defect is any error that, if not removed, could cause a software system to fail to meet its users' needs.
- Software quality is the degree to which a software product meets the needs of its users. Quality management focuses on defining, measuring, and refining the quality of the development process and the products developed during its various stages.
- Software developers are under extreme pressure to reduce the time to market of their products. They are driven by the need to beat the competition in delivering new functionality to users, to begin generating revenue to recover the cost of development, and to show a profit for shareholders.
- The resources and time needed to ensure quality are often cut under the intense pressure to ship a new software product. When forced to choose between adding more user features and doing more testing, many software companies decide in favor of more features.
- A business information system is a set of interrelated components—including hardware, software, databases, networks, people, and procedures—that collects and processes data and disseminates the output.
- Software product liability claims are typically based on strict liability, negligence, breach of warranty, or misrepresentation—sometimes in combination. Strict liability means that the defendant is held responsible for injuring another person regardless of negligence or intent.
- A warranty assures buyers or lessees that a product meets certain standards of quality and may be either expressly stated or implied by law. If the product fails to meet the terms of its warranty, the buyer or lessee can sue for breach of warranty.

What are some effective strategies for developing quality systems?

- A software development methodology is a standard, proven work process that enables systems analysts, programmers, project managers, and others to make controlled and orderly progress in developing high-quality software. Software methodologies define the activities in the software development process as well as the individual and group responsibilities for accomplishing objectives, recommend specific techniques for accomplishing the objectives, and offer guidelines for managing the quality of the products during the various stages of the development cycle.

- The waterfall system development model is a sequential, multistage system development process in which development of the next stage of the system cannot begin until the results of the current stage are approved or modified as necessary.
- Under the agile development methodology, a system is developed in iterations (often called sprints), lasting from one to four weeks. Agile development, which accepts the fact that system requirements are evolving and cannot be fully understood or defined at the start of the project, concentrates on maximizing the team's ability to deliver quickly and respond to emerging requirements.
- Using an effective development methodology enables a manufacturer to produce high-quality software, forecast project-completion milestones, and reduce the overall cost to develop and support software. An effective development methodology can also help protect software manufacturers from legal liability for defective software in two ways: by reducing the number of software errors that could cause damage and by making negligence more difficult to prove.
- The cost to identify and remove a defect in the early stages of software development can be up to 100 times less than removing a defect in a piece of software that has been distributed to customers.
- Quality assurance (QA) refers to methods within the development process that are designed to guarantee reliable operation of a product. Ideally, these methods are applied at each stage of the development cycle.
- There are several tests employed in software development including black-box and white-box dynamic testing, static testing, unit testing, integration testing, system testing, and user acceptance testing.
- Capability Maturity Model Integration (CMMI) models are collections of best practices that help organizations improve their processes. A best practice is a method or technique that has consistently shown results superior to those achieved with other means, and that is used as a benchmark within a particular industry. CMMI-Development (CMMI-DEV)—is frequently used to assess and improve software development practices.
- CMMI defines five levels of software development maturity: initial, managed, defined, quantitatively managed, and optimizing. CMMI identifies the issues that are most critical to software quality and process improvement. Its use can improve an organization's ability to predict and control quality, schedule, costs, and productivity when acquiring, building, or enhancing software systems. CMMI also helps software engineers analyze, predict, and control selected properties of software systems.
- A safety-critical system is one whose failure may cause human injury or death. In the development of safety-critical systems, a key assumption is that safety will *not* automatically result from following an organization's standard software development methodology.
- Safety-critical software must go through a much more rigorous and time-consuming development and testing process than other kinds of software; the appointment of a project safety engineer and the use of a hazard log and risk analysis are common in the development of safety-critical software.
- Risk is the potential of gaining or losing something of value. Risk can be quantified by three elements: a risk event, the probability of the event happening, and the impact (positive or negative) on the business outcome if the risk does actually occur.

- The annualized rate of occurrence (ARO) is an estimate of the probability that an event will occur over the course of a year. The single loss expectancy (SLE) is the estimated loss that would be incurred if the event happens. The annualized loss expectancy (ALE) is the estimated loss from this risk over the course of a year.
- The following equation is used to calculate the annual loss expectancy: ARO × SLE = ALE.
- Risk management is the process of identifying, monitoring, and limiting risks to a level that an organization is willing to accept.
- Reliability is a measure of the rate of failure in a system that would render it unusable over its expected lifetime.
- The International Organization for Standardization (ISO) issued its 9000 series of business management standards in 1988. These standards require organizations to develop formal quality management systems that focus on identifying and meeting the needs, desires, and expectations of their customers.
- The ISO 9001 family of standards serves as a guide to quality products, services, and management; it provides a set of standardized requirements for a quality management system. Many businesses and government agencies specify that a vendor must be ISO 9001 certified to win a contract from them.
- Failure mode and effects analysis (FMEA) is an important technique used to develop ISO 9001–compliant quality systems. FMEA is used to evaluate reliability and determine the effects of system and equipment failures.

Key Terms

acceptance
agile development
annualized loss expectancy (ALE)
annualized rate of occurrence (ARO)
avoidance
best practice
black-box testing
breach of warranty
business information system
Capability Maturity Model Integration (CMMI) models
CMMI-Development (CMMI-DEV)
contributory negligence
decision support system (DSS)
deliverable
dynamic testing
failure mode
failure mode and effects analysis (FMEA)
hazard log
high-quality software systems
integration testing
ISO 9001 family of standards
mitigation
N-version programming
product liability
quality assurance (QA)
quality management
redundancy
reliability
risk
risk management
safety-critical system
single loss expectancy (SLE)
software defect
software development methodology
software quality

static testing

strict liability

system safety engineer

system testing

transference

unit testing

user acceptance testing

warranty

waterfall system development model

white-box testing

Self-Assessment Questions

What is meant by software quality, why is it so important, and what potential ethical issues do software manufacturers face when making decisions that involve trade-offs between project schedules, project costs, and software quality?

1. Which one of the following statements is not true about high-quality software systems?
   a. They are easy to learn and easy to use.
   b. The need for such systems is a fairly recent occurrence.
   c. They operate quickly and efficiently.
   d. They keep system downtime to a minimum.

2. A software _____________ is any error that, if not removed, could cause a software system to fail.

3. Which one of the following is not a major cause of poor software quality?
   a. Many developers do not know how to design quality into software or do not take the time to do so.
   b. Many software developers are incompetent or lazy.
   c. Software developers are under extreme pressure to reduce the time to market of their products.
   d. Programmers make mistakes in defining system requirements.

4. _____________ focuses on defining, measuring, and refining the quality of the development process and the products developed during its various stages.

5. _____________ means that the defendant is held responsible for injuring another person, regardless of negligence or intent.
   a. Product liability
   b. Strict liability
   c. Negligence
   d. Contributory negligence

What are some effective strategies for developing quality systems?

6. A standard, proven work process that enables systems analysts, programmers, project managers, and others to make controlled and orderly progress in developing high-quality software is called a software _____________ .

7. The cost to identify and remove a defect in an early stage of software development is typically much less than the cost of removing a defect in an operating piece of software after it has been distributed to many customers. True or False?

8. A system development methodology in which systems are developed in iterations, often called “sprints,” lasting from one to four weeks is called ______________ development.

9. A software-testing technique in which the software is tested without actually executing the code is ______________.

   a. dynamic testing

   b. white-box testing

   c. static testing

   d. black-box testing

10. ______________ is a collection of best practices that help organizations assess and improve their software development practices.

    a. FMEA

    b. CMMI-DEV

    c. ISO 9000

    d. DOD-178B

11. If the annualized rate of occurrence is one percent and the annual loss expectancy is $100,000, the single loss expectancy is ______________.

    a. $1,000

    b. $10,000

    c. $100,000

    d. $10 million

12. The provision of multiple interchangeable components to perform a single function to cope with failures and errors is called ______________.

    a. risk

    b. reliability

    c. redundancy

    d. availability

13. ______________ is a measure of the rate of failure in a system that would render it unusable over its expected lifetime.

14. One of the most important and challenging areas of safety-critical system design is the system–human interface. True or False?

15. ______________ is an important technique used to develop ISO 9000–compliant quality systems by both evaluating reliability and determining the effects of system and equipment failures.

    a. N-version programming

    b. FMEA

    c. Redundancy

    d. Agile system development

Self-Assessment Answers

1. b.; 2. defect; 3. b.; 4. Quality management; 5. b.; 6. development methodology. 7. True; 8. agile; 9. c.; 10. b.; 11. d.; 12. c.; 13. Reliability; 14. True; 15. b

Discussion Questions

1. Identify the three criteria you consider to be most important in determining whether or not a system is a quality system. Briefly discuss your rationale for selecting these criteria.
2. What are the primary factors that contribute to poor-quality software? Which of these factors can be traced back to poor ethical decisions on the part of management or project team leaders or members?
3. Define quality management and quality assurance, and briefly discuss the difference between the two.
4. Explain why the cost to identify and remove a defect in the early stages of software development might be 100 times less than the cost of removing a defect in software that has been distributed to hundreds of customers. What are the implications for a software development organization?
5. Define the terms strict liability, negligence, contributory negligence, and breach of warranty, and explain how they differ.
6. Identify and briefly discuss two ways in which the use of an effective software development methodology can protect software manufacturers from legal liability for defective software.
7. Your company is considering using N-version programming—with three software development firms and three different hardware devices—for the navigation system of a guided missile. Briefly describe what this means, and outline several advantages and disadvantages of this approach.
8. Why is the system–human interface one of the most important and challenging areas of safety-critical systems? Do a search online and find three good sources of information relating to how to design an effective system–human interface.
9. Identify two commonly used system development methodologies. What are the primary pros and cons of each approach?
10. Identify and briefly describe six different forms of software testing.
11. What is the difference between system reliability and system safety? Give an example of a system that operates reliably but not safely.
12. Explain how an organization might use CMMI-DEV to improve its software development practices.
13. Identify and briefly discuss the implications to a project team of classifying a piece of software it is developing as safety critical.
14. What is risk? How can it be quantified? What problems might you encounter in trying to quantify risk?
15. What is risk management? Identify four strategies for addressing a particular risk.
16. What is the ISO 9001 family of standards? How does an organization achieve ISO 9001 certification? What are the benefits of such certification?
17. What is FMEA, and how is it used?

What Would You Do?

Use the five-step decision-making process discussed in Chapter 1 to analyze the following situations and recommend a course of action.

1. Read the fictional Killer Robot case at the website for the Online Ethics Center for Engineering at www.onlineethics.com/CMS/computers/compcases/killerrobot.aspx. The case begins with the manslaughter indictment of a programmer for writing faulty code that resulted in the death of a robot operator. Slowly, over the course of many articles, you are introduced to several factors within the corporation that contributed to the accident. After reading the case, answer the following questions:

   a. Responsibility for an accident is rarely defined clearly and is often difficult to trace to one or two people or causes. In this fictitious case, it is clear that a large number of people share responsibility for the accident. Identify all the people you think were at least partially responsible for the death of Bart Matthews, and explain why you think so.

   b. Imagine that you are the leader of a task force assigned to correct the problems uncovered by this accident. Develop a list of the six most significant actions to take to avoid future problems.

2. Your manager is leading a project to develop new software that is essential to the success of the midsized manufacturing firm where you work. The firm has decided to hire outside contractors to execute the project. One candidate firm boasts that its software development practices are at level 4 of CMMI. Another firm claims that all its software development practices are ISO 9001 compliant. Your manager has come to you and asked for your opinion on how much weight should be given to these certifications when deciding which firm to use. What would you say?

3. You are a programmer for a firm that develops a popular tax-preparation software package designed to help individuals prepare their federal tax returns. In the course of testing some small changes that were made to the software, you detect an error in the software that results in roughly a five percent underestimation of the amount owed—both for those who indicated that they were single and for those who indicated that they were married but filing separate tax returns. It is now late March, and it is likely that well over 100,000 users who submitted their returns using your firm's software will be affected by this error. What do you say to your firm's management?

4. You are the project manager in charge of developing the latest release of your software firm's flagship product. The product release date is just two weeks away, and enthusiasm for the product is extremely high among your customers. Stock market analysts are forecasting sales of more than $25 million per month. If so, earnings per share will increase by nearly 50 percent. There is just one problem: two key features promised to customers in this release have several bugs that would severely limit the software's usefulness. You estimate that at least six weeks are needed to find and fix the problems. In addition, even more time is required to find and fix 15 additional, less severe bugs just uncovered by the QA team. What would you recommend to management?

5. You have been assigned to manage software that controls the shutdown of the new chemical reactors to be installed at a manufacturing plant. Your manager insists the software is not safety critical. The software senses temperatures and pressures within a 50,000-gallon stainless steel vat and dumps in chemical retardants to slow down the reaction if it gets out of control. In the worst possible scenario, failure to stop a runaway reaction would result in a large explosion that would send fragments of the vat and spray caustic liquid flying for hundreds of yards in all directions.

Your manager points out that the human operators in charge of the reactor will be able to intervene in the case of a software failure to protect the plant employees and the surrounding neighborhood if the shutdown software failed. Besides, he argues, the plant is already more than a year behind its scheduled start-up date. He cannot afford the additional time required to develop the software if it is classified as safety critical. How would you work with your manager and other appropriate resources to decide whether the software is safety critical?

6. You are the CEO for a small, struggling software firm that produces educational software for high school students. Your latest software is designed to help students improve their SAT and ACT test scores. To prove the value of your software, a group of 50 students who had taken the ACT test were retested after using your software for four weeks. Unfortunately, there was no dramatic increase in their scores. A statistician you hired to ensure objectivity in measuring the results claimed that the variation in test scores was statistically insignificant. You had been counting on touting the results in the promotion of your new software.

   A small core group of educators and systems analysts will need at least six months to start again from scratch to design an improved product. Programming and testing could take another six months. Another option would be to go ahead and release the current version of the product and then, when the new product is ready, announce it as a new release. This would generate the cash flow necessary to keep your company afloat and save the jobs of 10 or more of your 15 employees. Given this information about your company's product, what would you do?

Cases

1. F-35 Plagued with Software Issues

The F-35 Joint Strike Fighter is a single-pilot, single-engine, combat jet with a precision, all-weather strike capability that uses a wide variety of air-to-surface and air-to-air weapons. It is designed as a stealth aircraft, with a top speed of Mach 1.6, radar-evading properties, and an array of sophisticated hardware and software systems. The F-35 is intended to replace several aging aircraft for the U.S. Air Force, U.S. Navy, and U.S. Marine Corps. Numerous allies of the United States have also placed orders for the F-35 with Lockheed Martin Aeronautics, which has partnered with several other aerospace companies to design and manufacture the fighter. There are three variants of the F-35—a conventional takeoff/landing aircraft, a short takeoff/vertical landing aircraft, and a version designed specifically for use with aircraft carriers. The F-35 program is the most expensive weapons program in history, with each aircraft costing in the neighborhood of $100 million each.

Despite its high profile and high cost, the F-35, which is sometimes referred to as a fifth-generation fighter, has been plagued by numerous software issues that impact its effectiveness as a state-of-the-art fighter aircraft:

- The software that controls the F-35's complex radar system keeps crashing, which means the radar often has to be rebooted in flight.
- The F-35's primary gun is a 25 mm rapid-fire cannon controlled by software that is behind schedule and may not be ready until years after the aircraft is scheduled to be deployed for action.
- The Autonomic Logistics Information System (ALIS) is designed to support the F-35's operations through its mission planning functions as well as via automated

maintenance scheduling and parts ordering. It is an extremely complex system, with 24 million lines of computer code, and it can take up to 24 hours for the data from one F-35 to sync up with an ALIS ground computer. A major software update intended to fix the myriad of defects impacting the performance of ALIS was not ready for the F-35's scheduled deployment by the Air Force in 2016, and it is unclear if it will be ready in time for the Navy's 2018 deployment. A DoD commissioned study found that schedule slippage and functionality problems with ALIS could lead to $20–$100 billion in additional costs for the F-35 program.

- Each F-35 has radar, video cameras, infrared sensors, and passive electronic warfare receivers that locate targets and threats in the air and on the ground. One of the most advanced features of the F-35 is that its computer system is intended to merge the information from all these sensors to create enhanced situational awareness through a simple combined-sensor display of each target or threat. Furthermore, this single display is intended to be shared instantly with every other plane in the attack group to provide all pilots with a more accurate and complete view of the target and the surrounding threat environment. This would eliminate the need for time-consuming radio voice exchanges. However, test pilots have reported their F-35s are creating false multiple tracks when all of their sensors are turned on. For example, when a radar and an infrared sensor detect the same enemy plane, the two sensors display it on the pilot's helmet-mounted sight as two enemy planes.

The Pentagon's F-35 Joint Program office has downplayed the severity of these issues, saying that it is aware of all the concerns and is currently working to address them. Lt. Gen. Chris Bogdan, the F-35's program executive officer, said in a statement, "While nearing completion, the F-35 is still in development and technical challenges are to be expected. The program has a proven track record of solving technical issues, and we're confident we'll continue to do so." According to Bogdan, "The F-35 Program has a dedicated effort underway to resolve or otherwise mitigate" all of the deficiencies raised in the October 2015 report by the director of operational test and evaluation for the U.S. Department of Defense.

However, at a time when more testing is desperately needed, the F-35 program is losing testing personnel, with test centers experiencing a turnover rate of approximately 20 percent with recent departures not being replaced. On top of that, program managers have started laying off maintenance staff, engineers, and analysts. The layoffs have triggered a cascading effect with remaining workers desperately searching for new employment before they are laid off.

Critical Thinking Questions

1. Do research to learn the current status of the F-35 fighter program. Document your findings in a two- or three-paragraph summary. What do you think are the most serious of the remaining software problems impacting the F-35?
2. Some say that it is unethical to deploy the F-35 prior to resolving all software issues that limit its effectiveness in combat or that could put the pilot at risk. Others say that the F-35 is an emerging, evolving piece of technology and that only through observation of its performance in combat can its various features be refined and perfected. State your opinion on this issue, and explain why you feel this way.

3. What suggestions do you have to improve the development and testing of the software for the F-35 fighter program?

Sources: "F-35 Joint Strike Fighter (JSF) Lightning II, Global Security," GlobalSecurity.org, www.globalsecurity.org/military/systems/aircraft/f-35.htm, accessed February 6, 2017; "F-35 Program Timeline," Lockheed Martin, https://www.f35.com/about/history, accessed February 6, 2017; David Martin, "Is the F-35 Worth It?," *60 Minutes*, February 16, 2014, www.cbsnews.com/news/f-35-joint-strike-fighter-60-minutes/; Judah Ari Gross, "If the F-35 Fighter Jet Is so Awesome, Why Is It so Hated?," *Times of Israel*, April 6, 2016, www.timesofisrael.com/if-the-f-35-fighter-jet-is-so-awesome-why-is-it-so-hated/; Ellie Zolfagharifard and Mark Prigg, "Controversial $400bn F-35 Fighter Jet Now Has Computer 'Brain' Problem Which Could See Entire Fleet Grounded," *Dailymail*, April 21, 2016, www.dailymail.co.uk/sciencetech/article-3552155/Controversial-F-35-fighter-jet-brain-problem-entire-fleet-grounded-claims-report.html; Zachary Cohen, "Pentagon Weapons Tester: F-35 Fighter Jet Has 'Significant' Problems," *CNN*, August 26, 2016, www.cnn.com/2016/08/26/politics/f-35-fighter-jet-problems-gilmore-memo/index.html; Dan Grazier and Mandy Smithberger, "F-35 May Never Be Ready for Combat," Project on Government Oversight, September 9, 2015, www.pogo.org/straus/issues/weapons/2016/f-35-may-never-be-ready-for-combat.html.

2. How Safe Are Self-Driving Cars?

According to the National Safety Council, an estimated 38,300 people were killed and another 4.4 million were injured as a result of accidents on U.S. roads in 2015. The vast majority of fatal accidents are due to human error, so self-driving vehicles have the potential to save a lot of lives. Indeed, one study estimated that widespread adoption of self-driving vehicles by the year 2030 could eliminate 90 percent of all auto accidents in the United States, thus eliminating close to $190 billion in auto repair and health care–related costs annually, and, even more importantly, saving thousands of lives.

The NHTSA recently adopted the Society of Automotive Engineers' levels for automated driving systems. The six levels range from complete driver control to full autonomy, as summarized below:

- Level 0 (no automation): A human driver controls it all: steering, brakes, acceleration, and the like, although the car may include some warning or intervention systems.
- Level 1 (driver assistance): Most functions are controlled by the human driver, but some specific functions (such as steering or accelerating) can be done automatically by the car.
- Level 2 (partial automation): These cars have at least one driver assistance system of "both steering and acceleration/deceleration using information about the driving environment" (such as cruise control or lane-centering) that is automated. The driver must still always be ready to take control of the vehicle, however, to handle "dynamic driving tasks."
- Level 3 (conditional automation): Drivers are able to completely shift "safety-critical functions" to the vehicle under certain traffic or environmental conditions. The driver is still present and is expected to "respond appropriately" if asked to intervene.
- Level 4 (high automation): At this level, cars are fully autonomous and are designed to handle all aspects of the dynamic driving task—even if a human driver does not respond appropriately to a request to intervene—including, performing all safety-critical driving functions and monitoring roadway conditions for an entire trip. However, it's important to note that this is limited to the "operational design domain" of the vehicle—meaning it does not cover every driving scenario.
- Level 5 (full automation): Cars at this level have a fully autonomous system that is designed to handle all aspects of the dynamic driving task under all the roadway and environmental conditions that could be managed by a human driver—

including extreme environments, such as on dirt roads (which are unlikely to be navigated by driverless vehicles in the near future).

Autonomous vehicles are chock full of sensors and cameras that observe, monitor, and record the surrounding environment, including other vehicles in the vicinity. All these data are fed into an artificial intelligence algorithm that makes decisions on what movements are right, wrong, safe, and unsafe for the car to perform given the conditions it is experiencing. Self-driving cars even have the ability to share their driving experiences and recorded data with other cars so that each car's computer can adapt its algorithm to the environments faced by other vehicles. The goal of this information sharing would be to improve the ability of all self-driving vehicles to react to situations on the road without actually having to experience those situations firsthand.

Tesla CEO Elon Musk, perhaps optimistically, anticipates the first fully autonomous Tesla to be ready by 2018 but expects that regulatory approval may require an additional one to three years. Audi, BMW, Fiat Chrysler, Ford, General Motors, Mercedes, Nissan, Toyota, Volvo, and Waymo (the new name of Google's self-driving division), all have some level of autonomous vehicle today, and all have plans to deliver a fully autonomous vehicle by 2025 or sooner.

Testing of autonomous vehicles has not been without incident, however. In 2016, one of Google's self-driving cars hit a bus during a test drive in California because the car made an incorrect assumption about how the bus would react in a particular situation. The vehicle had identified an obstruction on the road ahead, so it decided to stop, wait for the lane next to it to clear, and then merge into the other lane. Although the vehicle detected a city bus approaching in that lane, it made an incorrect assumption that the bus driver would slow down. The bus driver, however, assumed the car would stay put, so he kept moving forward. The car pulled out, hitting the side of the bus while going about 2 mph. This was the first time in several years of testing on public roads that a Google self-driving car caused a crash. Understanding why a crash involving a self-driving car occurred is important in order to avoid a repeat of that accident scenarios. In this case, Google made necessary changes to its software so that it would "more deeply understand that buses and other large vehicles are less likely to yield" than other types of vehicles.

A Tesla Model S with its autopilot system activated was involved in a fatal crash in 2016, the first known fatality in a Tesla in which autopilot was active. The accident occurred when a tractor trailer drove across the highway perpendicular to the Model S. Neither the driver nor the car noticed the big rig or the trailer "against a brightly lit sky," and the brakes were not applied. The vehicle's radar didn't help in this case because, according to Tesla, it "tunes out what looks like an overhead road sign to avoid false braking events." The NHTSA is investigating the accident to determine if the autopilot system was working properly; if not, it could consider ordering a recall to repair the problem.

Critical Thinking Questions

1. When self-driving cars are involved in accidents, where does liability reside? Is it the driver's fault? Is the car manufacturer or software manufacturer libel? How might the deployment of self-driving cars affect the insurance industry?
2. Some industry experts believe that the future of autonomous cars depends on the standardization of artificial intelligence algorithms across all vehicles. Such standardization would allow vehicles from different automobile manufacturers to share driving experience data and artificial intelligence algorithm updates. So, an adjustment like the one that Google made so its software would "more deeply understand that buses and other large vehicles

are less likely to yield" could be shared with other automakers. What are the pros and cons of implementing a standard artificial intelligence algorithm across all manufacturers? Do you think the vehicle manufacturers would accept this mandate? Why or why not?

3. Automated driving systems range from complete driver control (level 0) to full autonomy (level 5). Should the degree of care exercised in developing vehicle software increase as the level of autonomy increases, or should all vehicle software be treated with the same level of care? Explain your answer.

Sources: "Autonomous Car Forecasts," Driverless Future, www.driverless-future.com/?page_id=384, accessed February 9, 2017; Mark Prigg, "Can Self-Driving Cars Cope with Illogical Humans? Google Car Crashed because Bus Driver Didn't Do What It Expected," *Dailymail*, March 14, 2016, www.dailymail.co.uk/sciencetech/article-3491916/Google-admits-self-driving-car-got-wrong-Bus-crash-caused-software-trying-predict-driver-do.html; Jordan Golson, "Tesla Driver Killed in Crash with Autopilot Active, NHTSA Investigating," *The Verge*, June 30, 2016, www.theverge.com/2016/6/30/12072408/tesla-autopilot-car-crash-death-autonomous-model-s; Corinne Iozzio, "Who's Responsible When a Self-Driving Car Crashes?," *Scientific American*, May 1, 2016, https://www.scientificamerican.com/article/who-s-responsible-when-a-self-driving-car-crashes/; Paul, "When Autonomous Vehicles Crash, Is The Software Liable?," *Security Ledger (blog)*, October 11, 2013, https://securityledger.com/2013/10/when-autonomous-vehicles-crash-is-the-software-liable/; Chris Giarratana, "How AI Is Driving the Future of Autonomous Cars," *Read Write*, December 20, 2016, http://readwrite.com/2016/12/20/ai-driving-future-autonomous-cars-tl4; Alyson Shontell, "A Top Silicon Valley Investor Predicts that 2 Years from Now Everyone Will Be Chauffeured around in Driverless Cars on Highways," *Business Insider*, July 18, 2016, www.businessinsider.com/chris-dixon-future-of-self-driving-cars-interview-2016-6; Hope Reese, "Updated: Autonomous Driving Levels 0 to 5: Understanding the Differences," *Tech Republic*, January 20, 2016, www.techrepublic.com/article/autonomous-driving-levels-0-to-5-understanding-the-differences; "Automated Driving Levels of Driving Automation Are Defined in New SAE International Standard J3016," SAE International, https://www.sae.org/misc/pdfs/automated_driving.pdf, accessed March 7 2017; Mike Ramsey, "Self-Driving Cars Could Cut Down on Accidents, Study Says," *Wall Street Journal*, March 5, 2015, https://www.wsj.com/articles/self-driving-cars-could-cut-down-on-accidents-study-says-1425567905.

End Notes

[1] Susan Carey, "Delta Meltdown Reflects Problems with Aging Technology," *Wall Street Journal*, August 8, 2016, https://www.wsj.com/articles/delta-air-lines-says-computers-down-everywhere-1470647527.

[2] Damon Lavrinc, "A Brief History of Airline Software Screwups," *Wired*, April 17, 2013, https://wired.com/2013/04/airline-software-screw-ups/.

[3] Thom Patterson, "The Real Reason Airline Computers Crash," *CNN Tech*, August 8, 2016, http://money.cnn.com/2016/08/08/technology/delta-airline-computer-failure/index.html.

[4] Nick Bilton, "Nest Thermostat Glitch Leaves Users in the Cold," *New York Times*, January 13, 2016, https://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html?_r=0.

[5] Will Michaels and Frank Stasio, "Blue Cross Software Glitches Delay Claim Payments," *WUNC*, April 28, 2016, wunc.org/post/blue-cross-software-glitches-delay-claim-payments.

[6] Elizabeth Weise and Bart Jansen, "Software Update, Not Hackers, Caused Customs Computer Meltdown at Airports," *USA Today*, January 3, 2017, www.usatoday.com/story/tech/news/2017/01/03/border-outage-not-caused-hackers-customs-and-border-patrol-airlines-lines-airport/96107764/.

[7] Kate Murphy, "Do You Believe in God, or Is that a Software Glitch?," *New York Times*, August 27, 2016, https://www.nytimes.com/2016/08/28/opinion/sunday/do-you-believe-in-god-or-is-that-a-software-glitch.html.

[8] Ben Chelf, “Measuring Software Quality,” Coverity, www.coverity.com/library/pdf/open_source_quality_report.pdf, accessed February 19, 2017.

[9] Greg Finzer, “How Many Defects Are Too Many?,” Sogeti Labs, October 29, 2014, http://labs.sogeti.com/how-many-defects-are-too-many/.

[10] Venkata N. Inukollu, Divya D. Keshamoni, Taeghyun Kang, and Manikanta Inukollu, “Factors Influencing Quality of Mobile Apps: Role of Mobile App Development Life Cycle,” *International Journal of Software Engineering & Applications (IJSEA)* 5, no. 5 (September 2014), http://airccse.org/journal/ijsea/papers/5514ijsea02.pdf.

[11] Cecilia Rehn, “The Biggest Software Fails of 2016,” *Software Testing News*, January 10, 2017, http://www.softwaretestingnews.co.uk/biggest-software-fails-2016/.

[12] Martin Samson, *M. A. Mortenson Co. v. Timberline Software Co. et al.*, Internet Library of Law and Court Decisions, www.internetlibrary.com/cases/lib_case206.cfm, accessed March 23, 2013.

[13] Barry W. Boehm, “Improving Software Productivity,” IEEE *Computer* 20, no. 8 (1987): 43–58.

[14] Capers Jones, “Software Quality in 2002: A Survey of the State of the Art,” Technical Report, Software Productivity Research, Inc., November 2002.

[15] “CMMI Maturity Profile Report,” CMMI Institute, June 30, 2016, http://partners.cmmiinstitute.com/wp-content/uploads/2016/09/Maturity-Profile-Ending-Jun-30-2016.pdf.

[16] “100% of Honeywell’s Global Software Divisions Compatible with CMMI Maturity Level 5,” Honeywell, December 8, 2015, https://www.honeywell.com/newsroom/pressreleases/2015/12/100-of-honeywell-s-global-software-divisions-compatible-with-cmmi-reg-maturity-level-5.

[17] Jonathan P. Bowen, “The Ethics of Safety-Critical Systems,” *Communications of the ACM* 43 (2000): 91–97.

[18] Janet Leon, “The True Cost of a Software Bug: Part One,” Celerity Blog: Breakthroughs in Acceleration, February 28, 2015, http://blog.celerity.com/the-true-cost-of-a-software-bug.

[19] “7 Medical Device Failures Causing Serious Recalls,” Qmed, January 27, 2016, http://www.qmed.com/news/7-medical-device-failures-causing-serious-recalls.

[20] Shaun Nichols, “Airbag Bug Forces GM to Recall 4.3M Vehicles,” *The Register*, September 9, 2016, www.theregister.co.uk/2016/09/09/gm_recalls_airbags_software_bug/.

[21] Zachary Cohen, “Pentagon Weapons Tester: F-35 Fighter Jet Has ‘Significant’ Problems,” *CNN*, August 26, 2016, www.cnn.com/2016/08/26/politics/f-35-fighter-jet-problems-gilmore-memo/index.html.

[22] George C. Wilson, “Navy Missile Downs Iranian Jetliner,” *Washington Post,* July 4, 1988, www.washingtonpost.com/wp-srv/inatl/longterm/flight801/stories/july88crash.htm.

[23] “The ISO Survey of Management System Standard Certifications 2015,” ISO, www.iso.org/iso/iso-survey, accessed February 19, 2017.

[24] “Our Company,” Raytheon, www.raytheon.com/ourcompany, accessed March 28, 2013.

[25] “Enhance the Value You Provide to Raytheon and Our Customers,” Raytheon, www.raytheon.com/connections/supplier/r6s/fmea/index.html, accessed March 28, 2013.

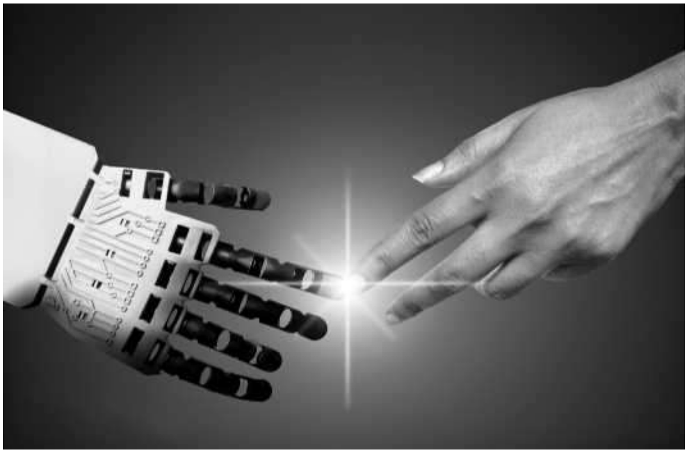
CHAPTER 8

THE IMPACT OF INFORMATION TECHNOLOGY ON SOCIETY

QUOTE

The number one benefit of information technology is that it empowers people to do what they want to do. It lets people be creative. It lets people be productive. It lets people learn things they didn't think they could learn before, and so, in a sense, it is all about potential.

—Steve Ballmer, former Microsoft CEO



Pixelbliss/Shutterstock.com

ORGANIZATIONS BEHAVING BADLY

An **electronic health record (EHR)** is a comprehensive view of the patient's complete medical history designed to be shared with authorized providers and staff from more than one organization. An EHR can include patient demographics, medical history, family history, immunization records, laboratory data, health problems, progress notes, medications, vital signs, and radiology reports.

Healthcare professionals can use an EHR to generate a complete electronic record of a clinical patient encounter, with the goal of ensuring that all information about a patient's medical history and ongoing treatment is easily accessible to all healthcare professionals involved in that patient's care—no matter where it occurs.

In 2005, the RAND Corporation predicted that if 90 percent of doctors and hospitals successfully adopted health information technology and used it effectively, resulting efficiencies would save $77 billion annually. Researchers also estimated that an additional $4 billion would be saved each year because of improved safety, primarily by reducing prescription errors as computerized systems warn doctors and pharmacists of potential mistakes.[1]

This prediction stimulated a major increase in investment in EHR and motivated the federal government to set aside up to $35 billion through the 2009 **Health Information Technology for Economic and Clinical Health Act (HITECH Act)** program to incentivize physicians and hospitals to implement such systems. Under this act, increased Medicaid and Medicare reimbursements are made to doctors and hospitals that demonstrate "meaningful use" of EHR technology.

To meet the meaningful use requirement, physicians must demonstrate that they are using EHR technology in ways that lead to significant and measurable results in achieving health and efficiency improvements, such as by e-prescribing medications and treatments, exchanging health information electronically, and submitting clinical quality data electronically to the Centers for Medicare and Medicaid Services (CMS). As of August 2015, the government had awarded over $28 billion to doctors and hospitals to install and use EHR systems from various software vendors.[2]

In 1996, Congress passed, and President Bill Clinton signed, the Health Insurance Portability and Accountability Act (HIPAA). One of its purposes was to smooth the transition, then just underway, from paper to electronic medical records. HIPAA called for the development of a unique identifier to be assigned to each individual. However, then-Representative Ron Paul (R-Texas), a libertarian with strong data privacy concerns, introduced language in the HIPAA legislation that barred the government from spending any money to develop such a unique identifier. Thus, the HIPAA law set a goal—and then blocked any progress toward it. Now, more than 20 years later, that prohibition still stands, causing ongoing issues related to electronic healthcare systems in the United States. Nationally, healthcare providers mismatch patients and their records 8 percent of the time on average. An EHR mismatch can result in issues ranging from a billing mistake to a catastrophic medical error.[3]

The HITECH Act was successful in increasing the percentage of U.S. hospitals using digital records—from 9.4 percent in 2008 to 75.5 percent in 2014.[4] But the U.S. healthcare system still lacks an easy, accurate, and reliable means to transfer an EHR medical file from one healthcare facility to another facility that uses an EHR system from a different vendor. As of August 2016, only 56 percent of hospitals had received electronic records from other practices in the past year—and just 40 percent of those had successfully merged that information into their own databases. Less than 10 percent of hospitals are able to trade records entirely using digital systems.[5] In addition, many physicians have concerns that use of an EHR system adds significant time to their workday—without improving the quality of care provided to patients.[6] Last, but not the least, the increased use of EHR systems places some 300 million patient records exposed to potential security lapses that can threaten the confidentiality, integrity, and availability of the data they contain.

What fundamental changes in laws and technologies must be made to make the transition to EHRs truly successful in the United States? Who must initiate these changes, and where will the needed resources come from?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What is the relationship between IT investment and productivity growth in the United States?
2. How will artificial intelligence, machine learning, robotics, and natural language processing affect the future workforce?
3. What impact has the application of IT had on health care?

THE IMPACT OF IT ON THE STANDARD OF LIVING AND WORKER PRODUCTIVITY

The standard of living varies greatly among groups within a country as well as from nation to nation. The most widely used measurement of the material standard of living is gross domestic product (GDP) per capita. National GDP represents the total annual output of a nation's economy. Overall, industrialized nations tend to have a higher standard of living than developing countries.

In the United States, as in most developed countries, the standard of living has been improving over time. However, its rate of change varies as a result of business cycles that affect prices, wages, employment levels, and the production of goods and services. Major disasters—such as earthquakes, hurricanes, tsunamis, and war—can negatively impact the standard of living. The worst economic downturn in U.S. history occurred during the Great Depression, when the GDP declined by about 50 percent from 1929 to 1932; by 1932, the unemployment rate had reached 25 percent.[7] By way of comparison, during the Great Recession in the United States (which began in 2007), the GDP growth rate declined by 6.8 percent during the fourth quarter of 2008 and the U.S. unemployment rate hit a peak of 10.2 percent in October 2009.[8,9]

IT Investment and Productivity

Labor productivity is a measure of economic performance that compares the amount of goods and services produced (output) with the number of labor hours used in producing those goods and services. Labor productivity is defined mathematically as real output per labor hour, and growth in labor productivity occurs when output increases faster than labor hours.

Most countries have been able to produce more goods and services over time—not through a proportional increase in labor but rather by making production more efficient. These gains in productivity have led to increases in the GDP-based standard of living because the average hour of labor produced more goods and services. The U.S. Department of Labor's Bureau of Labor Statistics tracks U.S. productivity on a quarterly basis. During the current business cycle, which started in the fourth quarter of 2007, U.S. labor productivity has grown at an annualized rate of 1.1 percent—less than half the average annual growth rate of 2.3 percent since 1947. This low rate of labor productivity growth is significant because increases in labor productivity mean that an economy is able to produce increasingly more goods and services for a given number of hours of work—making it possible for an economy to achieve growth in labor income and shareholder profits.[10]

Figure 8-1 shows the annual change in U.S. nonfarm labor productivity since 1948. The increase in productivity averaged 2.4 percent per year from 1948 to 1973 as modern management techniques and automation made workers far more productive. Productivity dropped off in the mid-1970s but rose again in the early years of the twenty-first century, only to drop dramatically to just above 1 percent from 2007 to 2016—a period of time corresponding to the deepest economic recession in the United States since the Great Depression.

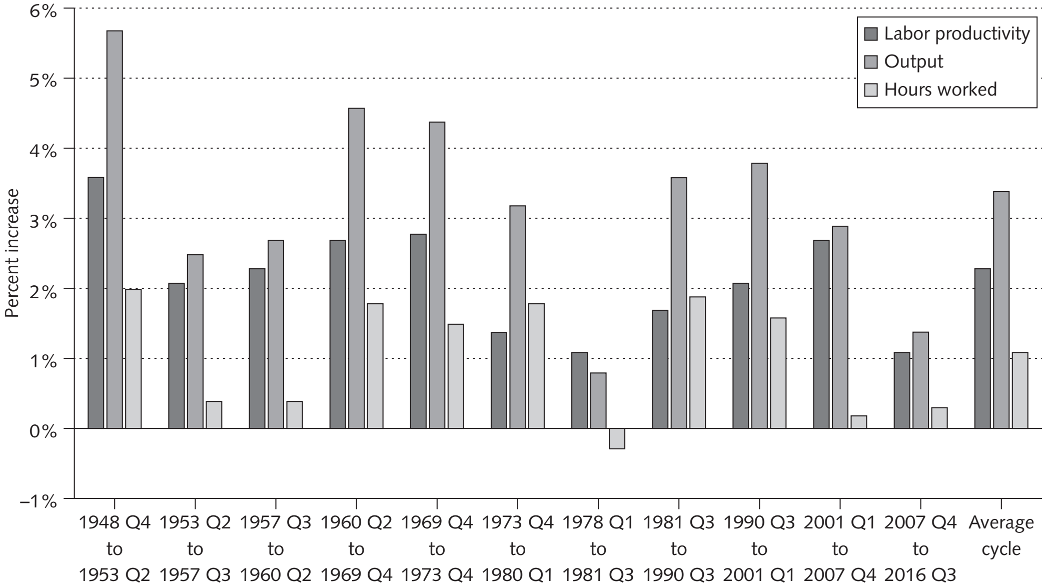


FIGURE 8-1 U.S. nonfarm labor productivity, 1948–2016

Source: U.S. Department of Labor BLS, https://www.bls.gov/opub/btn/volume-6/below-trend-the-us-productivity-slowdown-since-the-great-recession.htm, accessed February 26, 2017.

Innovation is a key factor in productivity improvement, and IT has played an important role in enabling innovation. Organizations use IT, as well as other new technology and capital investment, to implement innovations in products, processes, and services. In the early days of IT in the 1960s, productivity improvements were easy to measure. For example, midsized companies often had a dozen or more accountants focused solely on payroll-related accounting. When businesses implemented automated payroll systems, fewer accounting employees were needed. The productivity gains from such IT investments were obvious.

Today, organizations are trying to further improve IT systems and business processes that have already gone through many rounds of improvement. Organizations are also adding new IT capabilities to help workers who already have an assortment of personal productivity applications on their desktop computers, laptops, and smartphones. Instead of eliminating workers, IT enhancements are saving workers small amounts of time each day. Whether these saved minutes actually result in improved worker productivity is a matter for debate. Many analysts argue that workers merely use the extra time to do some small task they didn't have time to do before, such as responding to an email they would have otherwise ignored. These minor gains make it harder to quantify the benefits of today's IT investments on worker productivity. The relationship between investment in information technology and U.S. productivity growth is more complex than you might think. Consider the following facts:

- The rate of productivity from 1990 to 2000 of 2.1 percent is only slightly higher than the long-term U.S. rate of 2 percent and not nearly as high as it was during the 26 years following World War II. So, although the increase in productivity was welcome, it is not statistically significant.
- Labor productivity in the United States increased despite a reduced level of investment in IT from 2000 to 2007. If there were a simple, direct relationship, the labor productivity rate should have decreased.[11]

One possible explanation for the previous points is that there is a lag time between the application of innovative IT solutions and the capture of significant productivity gains. IT can enhance productivity in fundamental ways by allowing firms to make radical changes in work processes, but such major changes can take years to complete because firms must make substantial complementary investments in retraining, reorganizing, changing reward systems, and the like. Furthermore, the effort to make such a conversion can divert resources from normal activities, which can actually reduce productivity—at least temporarily. For example, researchers examined data from 527 large U.S. firms from 1987 to 1994 and found that it can take five to seven years for an IT investment to result in a substantial increase in productivity.[12]

Another explanation for the complex relationship between IT investment and U.S. productivity growth lies in the fact that many other factors influence worker productivity rates besides IT—the overall economic climate (expansion versus contraction); the flexibility of the labor market; the actions taken by private industry, various government entities, and the financial sector; and changes in supply and demand. Table 8-1 summarizes fundamental ways in which companies can increase productivity.

TABLE 8-1 Fundamental Drivers for Productivity Performance

Reduce the amount of input required to produce a given output by:	Increase the value of the output produced by a given amount of input by:
Consolidating operations to better leverage economies of scale	Selling higher-value goods and services
Improving performance by becoming more efficient	Selling more goods and services to increase capacity and use of existing resources

The following list summarizes additional factors that can affect national productivity rates:

- Labor productivity growth rates differ according to where a country is in the business cycle—expansion or contraction. Times of expansion enable organizations to gain full advantage of economies of scale and full production. Times of contraction present fewer investment opportunities.

- Outsourcing can skew productivity if the contracting firms have different productivity rates than the outsourcing firms.
- Regulations make it easier for companies in the United States to hire and fire workers and to start and end business activities compared to many other industrialized nations. This flexibility makes it easier for U.S. markets to relocate workers to more productive firms and sectors.
- More competitive markets for goods and services can provide greater incentives for technological innovation and adoption as firms strive to keep ahead of competitors.
- It can be difficult to measure the real output of such services as accounting, customer service, and consulting that make up a significant portion of today's service-based economy.
- IT investments don't always yield tangible results, such as cost savings and reduced head count; instead, they may produce intangible benefits, such as improved quality, reliability, and service.

As you can see, it is difficult to precisely quantify how much the use of IT has contributed to worker productivity. Ultimately, however, the issue is academic. There is no way to compare organizations that don't use IT with those that do, because there is no such thing as a noncomputerized airline, financial institution, manufacturer, or retailer.

Businesspeople analyze the expected return on investment to choose which IT option to implement, but at this point, trying to measure its precise impact on worker productivity is like trying to measure the impact of telephones or electricity.

CRITICAL THINKING EXERCISE: PRODUCTIVITY GROWTH—WHAT DIFFERENCE DOES IT MAKE?

Why is important for an organization to raise its output per worker over the long term? What happens if it cannot keep pace with the productivity growth of other organizations within the same industry? Identify several reasons why various companies within the same industry are likely to have significant differences in productivity growth.

IT AND WORKPLACE AUTOMATION

Advances in artificial intelligence, machine learning, robotics, and natural language processing are fundamentally changing the way work gets done and have the potential to affect the tasks, roles, and responsibilities of most workers. Computers and robots can perform a wide range of routine physical work activities better, cheaper, faster, and more safely than humans. They are also increasingly capable of accomplishing activities once considered impossible to automate successfully, such as working collaboratively with other machines, recognizing humans and objects, and even driving vehicles. Workplace automation is no longer a topic of science fiction; it is part of our everyday world. Global management consulting firm McKinsey & Company forecasts that productivity growth from the adoption of artificial intelligence, machine learning, and robotics will average between 0.8 percent and 1.4 percent per year between 2015 and 2065.[13]

One way to assess the feasibility of automating all or a portion of a job is to consider the multiple types of activity that make up that job. Almost every job has partial automation potential, and research suggests that 45 percent of human work activities could be automated using *existing* technology. Interestingly, this research also concludes that less than 5 percent of jobs can be *fully* automated—suggesting that workers will be augmented by automation, not replaced.[14]

The types of work-related activities most amenable to automation are physical tasks performed in highly structured and predictable environments (for example, mopping a floor, welding, or painting a part on an assembly line), as well as activities related to data collection and processing. Other activities suited to automation include many tasks in the accommodation and food service industries, almost half of all labor time involves predictable physical activities such as preparing, cooking, or serving food; collecting dirty dishes; providing room service; and cleaning guest rooms. Many activities in the manufacturing and retail industries are suitable for automation. The types of work-related activities least suited for automation include activities associated with managing others, applying expertise in making decisions and offering recommendations, interacting with stakeholders, and performing physical activities in an unstructured and unpredictable environment.[15]

It is likely to take decades for automation to achieve anywhere near its full potential. Consistent with E.M. Rogers' diffusion of innovation theory, the rate at which activities become automated and workers are affected will vary across different activities, occupations, and wage and skill levels. Each sector will have its innovators and its laggards.[16]

Artificial Intelligence

Computers were originally designed to perform simple mathematical operations, using fixed programmed rules and eventually operating at millions of computations per second. When it comes to performing mathematical operations quickly and accurately, computers beat humans hands down. However, computers still have trouble recognizing patterns, adapting to new situations, and drawing conclusions when not provided complete information—all activities that many humans can perform quite well. Artificial intelligence systems tackle these sorts of problems. **Artificial intelligence systems** include the people, procedures, hardware, software, data, and knowledge needed to develop computer systems and machines that can simulate human intelligence processes, including learning (the acquisition of information and rules for using the information), reasoning (using rules to reach conclusions), and self-correction (using the outcome from one scenario to improve its performance on future scenarios).

Artificial intelligence is a complex and interdisciplinary field in which experts ponder philosophical issues such as the nature of the human mind and the ethics of creating objects gifted with human-like intelligence. Artificial intelligence includes several specialty areas, including machine learning systems, robotics, and natural language processing. These areas are interrelated; advances in one can occur simultaneously with or result in advances in others.

Machine Learning

Machine learning, a type of artificial intelligence (AI), involves computer programs that can learn some task and improve their performance with experience. Machine learning systems consist of three major components: a model, parameters, and the learner (see Figure 8-2). Input is fed into the model, which makes a prediction. The learner component of the system compares the prediction with reality and uses the difference between the two to modify the parameters that are used in the model. This learning process is repeated until the learning system is able to make predictions that are sufficiently accurate.

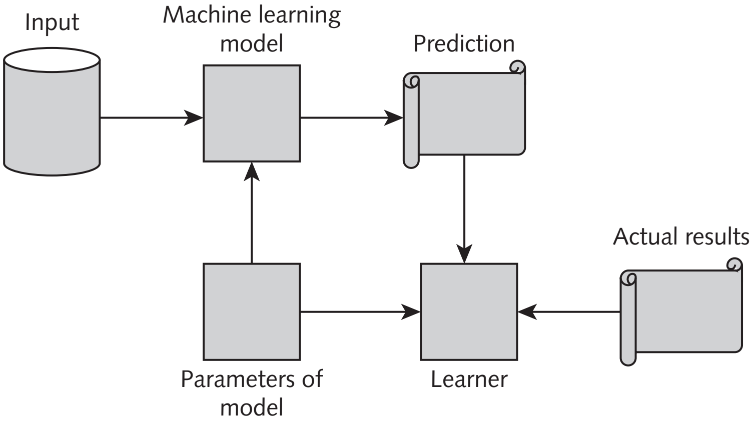


FIGURE 8-2 Components of a machine learning system

Machine learning is employed in a wide spectrum of computing functions in which designing and programming explicit algorithms is not feasible. Machine learning has contributed to the development of a much more in-depth understanding of the human genome as well as practical speech recognition, improved web search results, and self-driving cars. Machine learning is also used on websites to recommend other products a shopper might like based on what he or she has already purchased. In the financial services industry, machine learning is used to compare in-process credit card transactions to an existing database of transactions to detect fraud. And when your robot vacuum cleaner vacuums a room, machine learning helps it decide whether the job is done.

Autonomous vehicles use sophisticated radar systems and multiple cameras and sensors to recognize and adapt to a rapidly changing environment. Self-driving vehicles must accurately identify objects—is that another vehicle, an animal, a pedestrian, or debris in the road ahead? The key is a sophisticated machine learning system into which is fed many images containing objects. The model portion of the system examines the images and predicts what kind of object is in each one. Initially, many of its predictions will be wrong. However, the learner component of the learning system modifies the model parameters based on the difference between its initial misjudgments and reality, and then tries again. This prediction-feedback-modification training process continues, and the parameters are adjusted until the model correctly classifies all images. Afterward, new images are presented to the learning system, which will, ideally, classify them with a high degree of accuracy. If not, another round of training may be required.

IBM Watson is a cognitive computing system that can learn and reason based on interactions with humans, computer files, online interactions, and its environment. Natural language processing is a key ingredient as it enables Watson to recognize significant content within both written and spoken language. Watson also employs machine learning so that it can improve its performance based on experience and without benefit of human instruction.[17] Named after a former IBM CEO, Watson is aimed at bringing **artificial intelligence** to the general business world. Rather than selling Watson as a single system, IBM has broken down its capabilities into different components including the following: Watson virtual assistant for customer self-help, Watson explorer for high-powered enterprise-wide search, Watson analytics for data analysis and visualization, and Watson knowledge studio to gain insights from unstructured text.

H&R Block tax preparers and IBM development teams are training IBM Watson to master the 74,000 pages of the U.S. tax code. With this knowledge—and its ability to understand context, interpret intent, and draw connections—Watson will then be able to listen in on a tax-preparation interview with a human tax preparer and a client, and then suggest credits and deductions that might apply to the taxpayer.[18]

IBM is working with an alliance of some three dozen U.S. companies to help member companies choose the doctors and drugs that provide the best value to patients. Watson is being fed four years of data from each company, including EHRs and pharmacy and insurance claims. Once this data is digested, the goal is for Watson to make recommendations based on which doctors and drugs resulted in the best healthcare outcome for patients.[19]

Robotics

Robotics is a branch of engineering that involves the development and manufacture of mechanical or computer devices that can perform tasks that require a high degree of precision or that are tedious or hazardous for human beings, such as painting cars or making precision welds. Robots are often used to lift and move heavy pallets in warehouses, vacuum rooms, and inspect radioactively contaminated areas of power plants inaccessible by people.

The use of robots is expanding and is likely to continue to grow. Some people fear that robots will increasingly take jobs from human employees. For example, the use of autonomous vehicles may place millions of truck drivers, chauffeurs, and cab drivers out of work. Amazon employs 45,000 robots that automate the picking and packing process in 20 of its fulfillment centers. Each robot stands about 16 inches tall, weighs about 320 pounds, and is able to haul packages over twice its weight at up to 5 miles per hour.[20] Another area of particular interest is the use of robots as companions and caregivers for people who are sick, elderly, or physically challenged.[21] There is lingering concern, however, about whether an algorithm-driven robot can truly connect with people who feel lonely and are in need of meaningful social interaction.

Robots do not have the capacity to make moral judgments; these need to be programmed into them, which is a challenging task. The Quixote project at the Georgia Institute of Technology is breaking new ground by using stories to teach human values to robots. Quixote trains robots to read stories as a means of learning socially acceptable sequences of events and developing an understanding of appropriate ways to behave in human society. Suppose, for example, that a human were to ask a robot to pick up some groceries. A robot is generally designed to perform tasks in the most efficient and least costly manner possible, and so would speed recklessly to the store, run through aisles snatching up items, and bolt through the exit door without pausing to pay. With training from Quixote, the robot would know to proceed with caution, wait patiently in line at the checkout, and pay for the groceries.[22]

Natural Language Processing

Natural language processing is an aspect of artificial intelligence that involves technology that allows computers to understand, analyze, manipulate, and/or generate "natural" languages, such as English. Many companies provide natural language processing help over the phone. When you call a help phone number, you are typically given a menu of options and asked to speak your responses. Many people, however, become easily frustrated talking to a machine instead of a human. The Naturally Speaking application from Dragon Systems uses continuous voice recognition, or natural speech, that allows the user to speak to the computer at a normal pace without pausing between words. The spoken words are transcribed immediately onto the computer screen.

The Associated Press (AP) began using natural language processing to write its earnings reports, which summarize a company's business results. AP now generates some 3,000 earnings reports per quarter, ten times its previous output. Amazingly, the automated stories also contain fewer errors than stories written by actual journalists. The process starts with financial data from Zacks Investment Research and employs natural-language-generation algorithms to generate the stories. Automation has freed up reporters to work on more difficult stories, and, according to AP, no jobs have been eliminated as a result of the automated earnings reports.[23]

CRITICAL THINKING EXERCISE: POTENTIAL FOR AUTOMATION

What are the primary types of activities associated with your job? Which of these activities are most likely to be automated in the next 10 years? How do you think this might impact you?

THE IMPACT OF IT ON HEALTH CARE

The rapidly rising cost of health care is one of the twenty-first century's major challenges (see Figure 8-3). In 2015, U.S. healthcare spending hit an estimated $3.2 trillion, which was 17.8 percent of GDP, or an average of $9,990 per person. In 1960, healthcare costs were only $27.2 billion, just 5 percent of GDP, and only $146 per person.[24] U.S. healthcare spending is projected to grow at an average rate of 5.6 percent per year for the time period 2016–2025. This is a growth rate of 1.2 percentage points faster than GDP growth, meaning that the healthcare share of GDP is expected to rise from 17.8 percent in 2015 to 19.9 percent by 2025, according to the Centers for Medicare and Medicaid Services.[25]

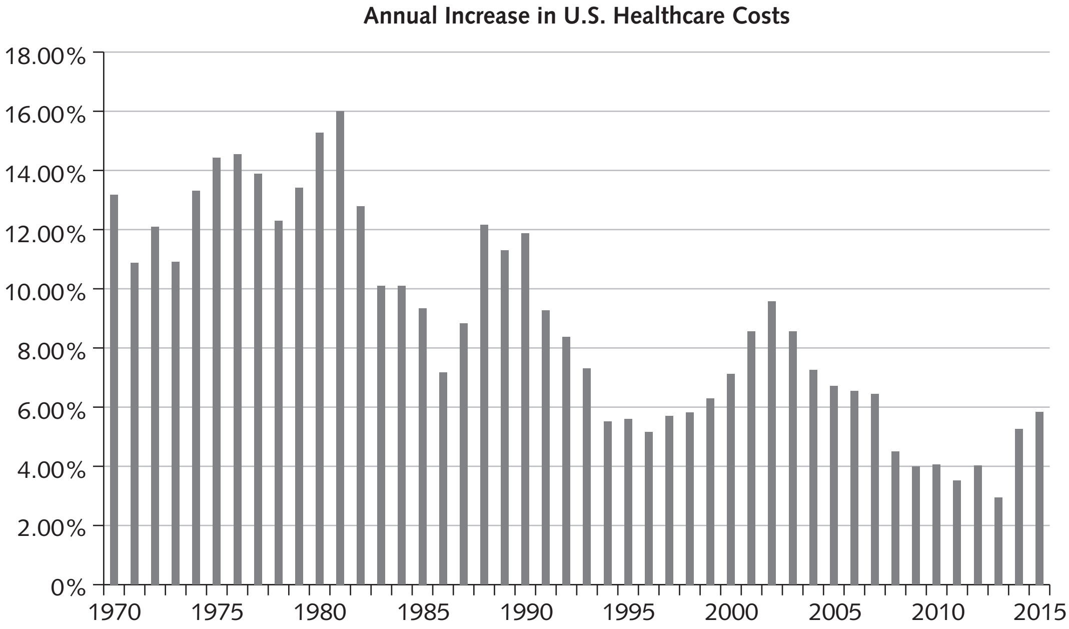


FIGURE 8-3 Annual increase in U.S. healthcare costs

Source: Peterson-Kaiser Health System Tracker, http://www.healthsystemtracker.org/interactive/health-spending-explorer/?display=U.S.%2520%2524%2520Billions&service=All%2520Types%2520of%2520Services.

Much of the increase in health care is due to three causes: the continued aging of the population in the United States, government policy, and lifestyle changes:

- The baby boom generation is heading into retirement, with enrollment in Medicare growing by over 1.6 million people annually. And as we get older, we tend to need more medical care and incur medical expenses.
- The Federal government created Medicare and Medicaid in 1965 to help those who were without insurance. These programs stimulated demand for healthcare services, and with increased demand came increased costs charged for those services. In addition, new groups of people were covered under these and
  other new programs, such as the Medicare Prescription Drug Plan (Part D), the Children's Health Insurance Plan, and the Affordable Care Act (ACA).
- Lifestyle changes have led to an increase in chronic illnesses, such as diabetes and heart disease, that are expensive and difficult to treat. The treatment of all types of chronic illnesses accounts for 85 percent of healthcare costs.

The development and use of new medical technology, such as new diagnostic procedures and treatments, also contributes to the increase in healthcare spending per person.[26] Although many new diagnostic procedures and treatments are at least moderately more effective than their older counterparts, they are also costlier. In addition, even if new procedures and treatments cost less (for example, magnetic resonance imaging), they may stimulate much higher rates of use because they are more effective or cause less discomfort to patients.

In order for the United States to rein in healthcare spending, patient awareness must be raised and technology costs must be managed more carefully. In the meantime, however, the increased use of IT in the healthcare industry has led to significant improvements in the quality of healthcare. The primary areas where IT has been applied include computerized patient records, clinical decision support, computerized provider order entry, and telehealth.

Computerized Patient Records

An **electronic medical record (EMR)** is a collection of health-related information on an individual that is created, managed, and consulted by authorized clinicians and staff within a single healthcare organization. It is a single practice's digital version of a patient's chart, containing the patient's medical history, diagnoses, and treatments. EMRs enable healthcare providers to track changes in patient healthcare data over time; identify patients due for vaccinations, screenings, or check-ups; and monitor key patient parameters such as blood glucose levels, blood pressure, and weight. The information in an EMR is not easily shared with others outside of the healthcare organization where the data originated. In fact, the patient's record might even have to be printed out and delivered in hard copy form to those outside the healthcare organization.

An EHR, on the other hand, is a comprehensive view of the patient's complete medical history designed to be shared with authorized providers and staff from more than one organization. EHRs capture data on the total health of the patient and include more than just the standard clinical data collected in the provider's office thus enabling a broader view of a patient's care.

Over the course of treatment for a serious injury or chronic disease, patient data might accumulate at a variety of locations, including their primary care physician's office and the offices of various specialists as well as multiple labs, pharmacies, hospitals, and emergency departments. The data are collected for multiple purposes, including direct patient care, provider reimbursement, and clinical research. These data may be stored in various systems using different formats employing different database technologies and information models. And despite the growing use of standard terminologies in health care, the same concept (for example, blood glucose) may be represented in a variety of ways from one setting to the next.

Health information exchange (HIE) is the process of sharing patient-level electronic health information between different organizations. HIE can result in more cost-effective and higher-quality care. For example, HIE can reduce expensive redundant tests that are ordered because one provider does not have access to the clinical information stored at another provider's location.

The key to electronic exchange is the standardization of health data. Once standardized, the data can be transmitted electronically to specialists, hospitals, labs, imaging facilities, emergency rooms, and pharmacies, with subsets of the data shared with insurance companies, government agencies, patients, and employers. With more complete patient information, providers improve their ability to make well-informed treatment decisions quickly and safely.

A **personal health record (PHR)** includes those portions of the EHR that are routinely shared with the patient—such as personal identifiers, contact information, health provider information, problem list, medication history, allergies, immunizations, and lab and test results. A PHR can exist either as a stand-alone application that allows information to be exported to or imported from other sources or as a "tethered" application connected to a specific healthcare organization's information system. Tethered PHRs (patient portals) enable patients to view, but not change, data from the provider's EHR. Some applications also allow patients to communicate electronically with their providers.

Table 8-2 provides a summary of the benefits of EHRs, EMRs, PHRs, and HIEs.

TABLE 8-2 Benefits of EHRs, EMRs, PHRs, and HIEs

Benefits for providers	Benefits for patients	Benefits for insurance companies
Quick access to patient records from inpatient and remote locations, for more coordinated, efficient care	Reduced need to fill out the same forms at each office visit	Lower healthcare costs as a result of reduced care redundancies and readmissions
Enhanced decision support, clinical alerts, reminders, and medical information	Reliable point-of-care information and reminders notifying providers of important health interventions	More efficient and accurate allocation of costs for services
Performance-improving tools and real-time quality reporting	Convenience of e-prescriptions electronically sent to pharmacy	
Legible, complete documentation that facilitates accurate coding and billing	Patient portals with online interaction with providers	
Interfaces with labs, registries, and other EHRs	Electronic referrals allowing easier access to follow-up care with specialists	
Safer, more reliable prescribing		

A primary care practice with four providers in two office locations in New York City offers a weight loss program and uses its EHR system to track key health indicators, such as weight, blood pressure, and cholesterol levels for roughly 400 patients participating in the program. Patients can view this data and keep track of their progress through a patient portal. Since joining the weight loss program, a number of patients have experienced substantial health improvements, including reductions in blood glucose and cholesterol levels. Some patients with chronic conditions have even been able to reduce or stop taking some of their medications.[27]

EHR systems and HIE hold great promise in improving the quality of care and reducing healthcare costs through their support for clinical decision support tools and computerized provider order entry systems.

Clinical Decision Support

Clinical decision support (CDS) is a process and a set of tools designed to enhance healthcare-related decision making through the use of clinical knowledge and patient-specific information to improve healthcare delivery. Effective use of CDS systems increases the quality of patient care while at the same time cutting costs. CDS can also help prevent errors and adverse events and boost provider and patient satisfaction.

CDS systems provide physician, staff, or other individuals with knowledge and patient-specific information, presented at appropriate times, to enhance health care. One example of a CDS is a drug-allergy interaction alert provided to a physician at the time of prescription order entry—thus reducing the likelihood of an adverse drug reaction. Another example is a CDS that suggests that the provider conduct certain tests or administer certain vaccinations based on the data that it finds in the patient's EHR.

AltaMed Health Services is comprised of 26 clinical locations that provide a wide range of services including primary care, family practice, general medicine, OB/GYN, pediatrics, cardiology, urology, and orthopedic services to 180,000 patients per year. AltaMed modified its preventive screening protocol and EHR system to monitor performance on 14 Healthcare Effectiveness Data and Information Set (HEDIS) quality metrics. Under the new protocol, when a medical assistant receives a preventive-screening alert as he or she is reviewing a patient's EHR, the assistant can initiate a lab order without obtaining authorization from the physician. As a result, AltaMed vastly improved its performance on all fourteen quality metrics, particularly screening for breast cancer, colorectal screening, diabetes, and depression. The new workflow not only saves time and improves healthcare quality, but it also helps AltaMed ensure its patients get preventive screening.[28]

More advanced artificial-intelligence-based clinical decision support systems can help doctors choose the proper dosage levels of medication based on a patient's most recent tests results, assist radiologists in identifying tumors and other diseases, and recommend which surgical options are likely to yield the best outcomes. For example, developers built a decision-making algorithm that can be applied to an ultrasound image of a breast lesion to generate a recommendation about whether a biopsy should be performed.

Computerized Provider Order Entry

A **computerized provider order entry (CPOE) system** enables physicians to place orders (for drugs, laboratory tests, radiology, physical therapy) electronically, with the orders transmitted directly to the recipient. CPOE streamlines the ordering process because lab techs, nurses, and pharmacy staffs do not need to seek clarification or solicit missing information due to illegible or incomplete orders.

More than 7 million serious, potentially avoidable medication errors occur annually.[29] In hospital-related settings, implementing CPOE is associated with a greater than 50 percent decline in preventable adverse drug effects.[30]

Telehealth

Telehealth employs electronic information processing and telecommunications to support at-a-distance health care, provide professional and patient health-related training, and support healthcare administration. The Internet, broadband, and wireless technologies;

smartphones; laptop and tablet computers; videoconferencing; streaming media; and store-and-forward, high-resolution imaging are technologies frequently used to support telehealth.

Telemedicine is the component of telehealth that provides medical care to people at a location different from the healthcare providers. Telemedicine helps reduce the need for patients to travel for treatment and allows healthcare professionals to serve more patients in a broader geographic area. Some 15 million people in the United States received healthcare services that included telemedicine in 2014, and it is estimated that that number grew to 20 million in 2016.[31] There are three basic forms of telemedicine: store-and-forward, live telemedicine, and remote monitoring.

Store-and-forward telemedicine involves acquiring data, sound, images, and video from a patient and then transmitting everything to a medical specialist for later evaluation. This type of monitoring does not require the presence of the patient and care provider at the same time. Yet, having access to such data can enable healthcare professionals to recognize problems and intervene with remote patients before high-risk situations become life threatening.

Today most radiologists employ store-and-forward telemedicine technology to review cases from a remote location. Physicians in the emergency department of hospitals, for example, can order images in the middle of the night and send them to a so-called nighthawk radiology service firm that employs several radiologists who are licensed in multiple states and who work in shifts around the clock. Store-and-forward telemedicine enables the radiology practice to handle a large case volume from around the country and still deliver their findings within minutes or, at most, a few hours.

Live telemedicine requires the presence of patients and healthcare providers at different sites at the same time and often involves a video conference link between the two sites. Doctors Without Borders (DWB) employs live telemedicine so that medical teams operating in the field under difficult circumstances in remote areas can consult with specialists located hundreds or even thousands of miles away. Between 2010 and 2015, DWB logged over 1,300 telemedicine cases from more than 240 referral sites around the globe, including some in the most impoverished nations in the world.[32]

Aleutian Pribilof Islands Association (APIA), a nonprofit tribal organization of the Aleut people located off the coast of Alaska, administers five regional health clinics that are roughly 800 miles away from the nearest hospitals or specialists in Anchorage. Extreme weather often causes flight cancellations, so many of APIA's patients find it difficult to travel to medical appointments with specialists on the mainland. To improve access to healthcare services for its members, APIA uses telehealth to enable patients to consult with specialists electronically. For example, a patient with a heart condition can go to one of APIA's local clinics and use its telehealth equipment to conduct a virtual meeting with a cardiologist. Data from an EKG device, blood pressure cuff, and other data-collection tools is securely and instantaneously transmitted from the clinic to a cardiologist in Anchorage. The cardiologist then uses this data to assess whether or not the patient needs an in-person appointment for follow-up. This enables APIA's patients to avoid unnecessary and costly travel while still receiving a high level of care.[33]

Remote monitoring (also called home monitoring) involves the regular, ongoing, accurate measurement of an individual's vital signs (temperature, blood pressure, heart rate, and breathing rate) and other health measures (for example, glucose levels for a diabetic) and the transmission of this data to a healthcare provider. Patients who have chronic diseases often don't recognize early warning signs that indicate an impending health crisis, but a physician using telemedicine to keep tabs on such a patient could be alerted to potentially life-threatening symptoms before a crisis occurs.

There are thousands of mobile applications available to improve patient's access to healthcare information and to enable doctors to keep a close watch on patients' conditions. Commonly used apps include those that provide appointment and prescription reminders, medication and vital-sign tracking, and diet and weight monitoring; such apps typically communicate healthcare information by sending text or email messages to the patient, the healthcare professional, or to a monitoring computer. For example, one iPhone app can measure your blood pressure and heart rate, timestamp and record the readings, and then email the data to a physician.[34] However, the Joint Commission on Accreditation of Healthcare Organizations has stated that it is not acceptable for medical professionals to communicate with patients via SMS text messages. HIPPA regulations could be violated if sensitive patient information is sent via standard text messages. This ruling is requiring mobile apps developers to avoid the use of SMS text messages and instead employ more secure communications methods.[35]

In the United States, about 130,000 people die each year from atrial fibrillation (AF), a common form of abnormal heart rhythm and a major cause of strokes. AliveCor, Biotricity, Preventice Solutions, and other companies offer heart-monitoring kits that record and send electrocardiogram (ECG) data wirelessly to a smartphone or smartwatch app or to the cloud so that doctors can be alerted immediately if a patient's heart is exhibiting abnormal electrical activity. Medical experts believe that such capability could save thousands of lives. Regulatory approval by the Food and Drug Administration of these devices is critical as doctors prefer clinically proven products whose data they can trust in making clinical decisions. However, the rigorous testing process required for a health product to receive regulatory approval can take years and millions of dollars, so many consumer tech companies don't bother.[36]

The use of telemedicine does raise some legal and ethical questions, including the following:

- Must the physicians providing advice to patients at a remote location be licensed to perform medicine in that location—perhaps a different state or country?
- Must a healthcare system be required to possess a license from a state in which it has a "virtual" facility, such as a video conferencing room?
- Will the various states require some form of assurance that minimum technological standards (such as the minimum resolution of network-transmitted images) are being met?
- What sort of system certification and verification is necessary to ensure that a critical system performs as expected in crises situations, and what are the ramifications if it does not?

In addition, recent studies have shown that there is reluctance on the part of many doctors and nurses for remote doctors to have anything more than minimal involvement with their patients. There is a concern that patient involvement with remote doctors may have a negative effect on the local doctors' relationships with their patients and could adversely affect patient care.[37]

CRITICAL THINKING EXERCISE: AUTOMATED CLINICIANS

It is the year 2024, and robots are being introduced to handle the screening of patients at physicians' offices across the United States. The robots are human looking and are able to speak and understand English and Spanish. The robots are capable of performing basic nursing tasks, such as taking a patient's vital signs. Upon arriving at a physician's office, a patient would meet with the robot to determine the patient's current conditions and symptoms and to review pertinent medical history from the patient's EHR. The robot would form a preliminary diagnosis and suggest a course of action, which could include additional tests, medication, referral to a specialist, or hospitalization. A human physician would then review the preliminary diagnosis and suggested course of action. If necessary, the physician would meet with the patient to confirm the robot's diagnosis and order any additional work or medications that might be necessary. The robotic physician assistant can be made available 24 × 7 and can even be stationed at convenient locations, such as shopping malls, schools, places of work, and college campuses. The goal of using of robotic physician assistants is to increase the number of patients that could be seen by a single physician, while also cutting patient wait time.

You are on the administrative staff of a large physician group that is among the first to introduce robotic physician assistants. What sort of testing is necessary before the automated clinician can be certified as fit for use? What start-up issues might be expected? What would you do to make the use of a robotic physician assistant more acceptable to patients and to ensure patient care does not suffer?

Summary

What is the relationship between IT investment and productivity growth in the United States?

- The most widely used measurement of the material standard of living is gross domestic product (GDP) per capita.
- In the United States, as in most developed nations, the standard of living has been improving over time. However, its rate of change varies as a result of business cycles that affect prices, wages, employment levels, and the production of goods and services.
- Labor productivity is a measure of the economic performance that compares the amount of goods and services produced with the number of labor hours used in producing those goods and services.
- Most countries have been able to produce more goods and services over time—not through a proportional increase in labor but rather by making production more efficient. These gains in productivity have led to increases in the GDP-based standard of living because the average hour of labor produced more goods and services.
- Innovation is a key factor in productivity improvement, and IT has played an important role in enabling innovation. Organizations use IT, other new technology, and capital investment to implement innovations in products, processes, and services.
- It can be difficult to quantify the benefits of IT investments on worker productivity because there can be a considerable lag between the application of innovative IT solutions and the capture of significant productivity gains. In addition, many factors other than IT influence worker productivity rates.

How will artificial intelligence, machine learning, robotics, and natural language processing affect the future workforce?

- Advances in artificial intelligence, machine learning, robotics, and natural language processing are fundamentally changing the way work gets done and have the potential to affect the tasks, roles, and responsibilities of most workers.
- Almost every job has partial automation potential and research suggests that 45 percent of human work activities could be automated using existing technology.
- It is likely to take decades for automation to achieve anywhere near its full potential.
- Artificial intelligence systems can simulate human intelligence processes, including learning, reasoning, and self-correction.
- Machine learning, a type of artificial intelligence (AI), involves computer programs that can learn some task and improve their performance with experience.
- Robotics is a branch of engineering that involves the development and manufacture of mechanical or computer devices that can perform tasks that require a high degree of precision or that are tedious or hazardous for human beings.
- Natural language processing is an aspect of artificial intelligence that involves technology that allows computers to understand, analyze, manipulate, and/or generate “natural languages” such as English.

What impact has the application of IT had on health care?

- Healthcare costs in the United States are expected to increase an average of 5.6 percent per year from 2016 to 2025.
- Much of this increase is due to the continued aging of the population, government policy, and life style changes, and to a lesser extent the development and use of new medical technology.
- In order for the United States to rein in healthcare spending, patient awareness must be raised and technology costs must be managed more carefully.
- An electronic medical record (EMR) is a collection of health-related information on an individual that is created, managed, and consulted by authorized clinicians and staff within a single healthcare organization. The information in an EMR is not easily shared with others outside of the healthcare organization where the data originated.
- An electronic health record (EHR) is a comprehensive view of the patient's complete medical history designed to be shared with authorized providers and staff from more than one organization.
- Health information exchange (HIE) is the process of sharing patient-level electronic health information between different organizations. HIE can result in more cost-effective and higher-quality care.
- A personal health record (PHR) includes those portions of the EHR that an individual patient "owns" and controls such as personal identifiers, contact information, health provider information, problem list, medication history, allergies, immunizations, and lab and test results.
- Clinical decision support (CDS) is a process and a set of tools designed to enhance health-related decision making through the use of clinical knowledge and patient-specific information to improve healthcare delivery. Effective use of CDS systems increases the quality of patient care while at the same time cutting costs.
- A computerized provider order entry (CPOE) system enables physicians to place orders (for drugs, laboratory tests, radiology, physical therapy) electronically with the orders transmitted directly to the recipient. CPOE streamlines the ordering process.
- Telehealth employs modern telecommunications and information technologies to provide medical care to people who live or work far away from healthcare providers, provide professional and patient health related training, and support healthcare administration.
- Telemedicine is the component of telehealth that provides medical care to people at a location different from the healthcare providers. Telemedicine helps reduce the need for patients to travel for treatment and allows healthcare professionals to serve more patients in a broader geographic area.
- Store-and-forward telemedicine involves acquiring data, sound, images, and video from a patient and then transmitting everything to a medical specialist for later evaluation.

Key Terms

artificial intelligence systems

clinical decision support (CDS)

computerized provider order entry (CPOE) system

electronic health record (EHR)

electronic medical record (EMR)

health information exchange (HIE)

Health Information Technology for Economic and Clinical Health Act (HITECH Act)

labor productivity

live telemedicine

machine learning

natural language processing

personal health record (PHR)

remote monitoring

robotics

store-and-forward telemedicine

telehealth

telemedicine

Self-Assessment Questions

What is the relationship between IT investment and productivity growth in the United States?

1. U.S. nonfarm labor productivity from 1948 to 2016 has averaged about ____________ per year.
   - a. 1.1 percent
   - b. 2.3 percent
   - c. 3.0 percent
   - d. 3.3 percent
2. ____________ is the amount of output produced per unit of input.
3. The average annual growth rate of nonfarm labor productivity has never exceeded 3 percent. True or False?
4. A study of 527 large U.S. firms from 1987 to 1994 found that the benefits of applying IT grow over time and that an IT investment can take ____________.
   - a. one to three years to break even
   - b. three to five years for its users to become efficient in its use
   - c. five to seven years to result in a substantial increase in productivity
   - d. over seven years to fully recover the initial investment costs

How will artificial intelligence, machine learning, robotics, and natural language processing affect the future workforce?

5. Almost every job has partial automation potential, and research suggests that ____________ of human work activities could be automated using existing technology.
   - a. about 25 percent
   - b. almost one-third
   - c. 45 percent
   - d. well over half

6. The types of work activities least likely to be automated are activities related to ______________.
   a. data collection
   b. interactions with stakeholders
   c. data processing
   d. physical tasks performed in a structured and predictable environment
7. ______________ involves computer programs that can learn some task and improve their performance on that task with experience.
8. The rate at which activities become automated and workers are affected will vary across different activities, occupations, and wage and skill levels. True or False?

9. Which of the following is not one of the three main components of a machine learning system ______________?
   a. a model
   b. parameters
   c. the learner
   d. explanation facility

What impact has the application of IT had on health care?

10. Which of the following statements about healthcare spending is *not* true?
    a. Lifestyle changes have had a dramatic impact on increasing healthcare costs.
    b. Much of the growth in healthcare costs is due to the continued aging of the population in the United States.
    c. The development and use of new medical technology in the United States has clearly led to a reduction in healthcare costs.
    d. U.S. spending on health care is expected to increase on an average of 5.6 percent per year from 2016 until 2025.
11. Which of the following statements about electronic healthcare records is true?
    a. EHRs contain the health-related information of an individual from a single healthcare organization.
    b. The data in an EHR system from one EHR can always be easily shared electronically with a physician who uses an EHR system from another software vendor.
    c. A health information exchange can be helpful in sharing patient-level electronic information between different organizations.
    d. The data in an EHR is not intended to be shared with others outside the organization that collects the patient's data.
12. Clinical ______________ is a process and a set of tool designed to enhance healthcare-related decision making based on the use of clinical knowledge and patient-specific information to improve healthcare delivery.

13. A CPOE system enables physicians to place orders (for drugs, laboratory tests, radiology, physical therapy) electronically, with the orders transmitted directly to the recipient. True or False?

14. ______________ is the component of telehealth that provides medical care to people at a location different from the healthcare providers.

Self-Assessment Answers

1. b; 2. Labor productivity; 3. False; 4. c; 5. c; 6. b; 7. machine learning; 8. True; 9. d; 10. c; 11. c; 12. decision support; 13. True; 14. Telemedicine

Discussion Questions

1. We are undergoing a period of rapid technology change with cloud computing, artificial intelligence, robotics, mobile devices, wireless networks, and increasingly powerful computers; yet, U.S. labor productivity growth between 2007 and 2016 has been estimated to be an anemic 1 percent. What factors could help explain this low level of productivity?
2. Do research online to see how U.S. labor productivity growth compares to that in other countries. Create a simple graph, and write a brief paragraph to summarize your findings.
3. Some economists believe that the United States does not have a productivity problem but rather a measurement problem. Explain what is meant by this statement. Do you believe this is a valid statement?
4. Global management consulting firm McKinsey & Company forecasts that labor productivity growth from the adoption of artificial intelligence, machine learning, and robotics will average between 0.8 percent and 1.4 percent per year between 2015 and 2065. Does this estimate seem reasonable to you? Why or why not? What are the implications for the U.S. economy if this rate of productivity can be achieved?
5. Are there particular areas you think are ripe targets for the application of machine learning? What are they, and why do you think they could benefit from the application of machine learning?
6. What do you see as the role of robotics over the next decade? What is your most optimistic outlook? What is your most pessimistic outlook?
7. The development and use of new medical technology has increased healthcare spending. Should the medical industry place more emphasis on using older medical technologies and containing medical costs, or should the strategy be to use the latest and greatest technology available? Explain your answer.
8. The value of EHRs is being challenged by many in the healthcare industry. Why is this? In your opinion, is the investment in EHRs worth it? Why or why not?
9. What are some of the issues and concerns associated with the expanded use of telemedicine?
10. Can you imagine a breakthrough wearable remote monitoring device that could be used to not only detect emergency health conditions *before* they seriously impact the patient but also dispense life-saving medicine? Describe your device.

What Would You Do?

Use the five-step decision-making process discussed in Chapter 1 to analyze the following situations and recommend a course of action.

1. Your financial adviser wants you to allow his firm to manage your funds using a robo-investment adviser—an artificial intelligence software product that will constantly monitor your account 24 × 7 and make investment decisions consistent with your financial goals and the level of risk with which you are comfortable. The services fee will be reduced from your current 1.25 percent per year of total assets to 0.75 percent per year. What questions would you ask to decide if robo-investing was right for you?

2. It is 2025 and fully automated self-driving cars ("complete" with no steering wheel) are now widely available. In fact, such cars can be bought for only a $5,000 premium over traditional, nonautomated cars. You are in the market for a new car. Which model do you select—the autonomous or traditional model? Why?
3. You are a member of the IT organization at a full-service, nonprofit healthcare system that provides a wide range of clinical, educational, preventive, and social programs. These services are provided through two acute care hospitals and more than 130 sites of care. The healthcare system has a total of 12,000 employees, including almost 700 physicians. You have been asked to lead a project to assess the level of acceptance of the hospital's current EHR system. The goal is to establish whether or not the system is meeting employee's and patients' needs and, if not, define changes that need to be made, including requirements that must be met by any replacement system. Describe an effective approach to complete this effort. Develop a set of at least six questions that might be asked of various stakeholders to understand how and to what degree they currently use the EHR system as well as to determine their level of satisfaction.
4. You have volunteered to lead a group of local citizens in approaching the board of directors of the nearest hospital (55 miles away) about establishing remote monitoring of 25 or so chronically ill people in your small community in Alaska. How would you convince the board to support your community? What sort of facts do you need to gather to support your case? What specific services and support would you request?
5. You are a midlevel manager at a major metropolitan hospital and are responsible for capturing and reporting statistics regarding the cost and quality of patient care. You believe in a strict interpretation when defining various reportable incidents; as a result, your hospital's rating on a number of quality issues has declined during the six months you have held the position. Your predecessor was more lenient and was inclined to let minor incidents go unreported or to classify some serious incidents as less serious. The quarterly quality meeting is next week, and you know that your reporting will be challenged by the chief of staff and other members of the quality review board. How should you prepare for this meeting? Should you defend your strict reporting procedures or revert to the former reporting process for the "sake of consistency in the numbers," as several people have urged?

Cases

1. IBM Watson—Not Yet Ready for Prime Time?

The University of Texas MD Anderson Cancer Center is one of the world's most respected medical centers—devoted exclusively to cancer patient care, research, education, and prevention. Its 21,000 employees are focused on one mission: to end cancer. Each year, the center treats over 100,000 people, and it is currently running more than 1,200 clinical trials designed to test various types of cancer treatments.

In 2012, the center launched an ambitious project in collaboration with IBM to create the Oncology Expert Adviser (OEA), a learning system employing the IBM Watson cognitive computing program. OEA was designed to read and learn from MD Anderson's vast database of electronic medical records, academic literature, research data, and treatment options. In theory, OEA would glean patterns from all this data and use that knowledge to make suggestions to improve individual patient cancer care. In addition, OEA was intended to match cancer patients to appropriate clinical trials to offer patients an opportunity to fight their cancers by participating in trials of new therapies.

Unfortunately, after five years of effort (at a cost of $62 million), the center has not achieved its desired results, according to an assessment performed by the University of Texas System Audit Office. Incorporating machine learning software into complex healthcare settings is extremely challenging, and according to the audit report, the system never reached a development phase in which it could be used in a clinical setting. The audit uncovered project management failings as well as limitations in the program's ability to integrate with other hospital systems.

Initially, the OEA pilot project was focused on leukemia, but that effort was "suspended mid-project" because of lack of progress, and the project was refocused on lung cancer. The lung-cancer system was tested as a pilot project in 2015 and was able to suggest the same treatment plan as MD Anderson physicians in 90 percent of select cases. However, in order for the system to be useful in making complex healthcare-related recommendations, medical personal need to know how OEA reached a conclusion and what data and logic was used. A visualization tool called WatsonPaths attempted to fill this need; however, that tool was also complex, requiring a high level of technical sophistication to interpret how Watson arrived at its conclusion.

Another issue noted in the audit of the system is that the lung-cancer pilot was conducted using data from the hospital's old electronic records system, which was replaced in 2016, and the project team has been unable to integrate the pilot program with the hospital's current electronic health records. In addition, clinical trial and drug-protocol data in the OEA system are outdated. Before the program could be tested further, major rework would be required to first convert data from the old system to make it compatible with the new system, and then retrain OEA on all the data in the new records system.

Another goal of the project was to make OEA widely available to physicians at partner hospitals outside MD Anderson. However, the audit found that the program was never piloted with partner hospitals. The audit cited cybersecurity concerns and "lack of engagement or interest" by partner hospitals as factors that prevented the testing of the technology outside MD Anderson.

Defining a successful treatment plan for lung cancer is certainly a challenging task, more so than many other problems to which the computing power of Watson has been applied. OEA did not prove that vast amounts of patient data and knowledge of various courses of cancer treatment are as significant as advocates of artificial intelligence make them out to be. MD Anderson and the OEA project still needs to provide evidence that the technology could be developed to a level at which it would reliably improve patient outcomes, lower costs, or provide some other benefit.

Critical Thinking Questions

1. As noted in the case, the OEA pilot system was tested in 2015 and was able to suggest the same treatment plan as MD Anderson physicians on 90 percent of select cases. Should MD Anderson accept this degree of accuracy? How should it determine an acceptable level of accuracy for such a system?
2. What key learnings did MD Anderson gain from this effort that may influence future efforts?
3. Should MD Anderson personnel have known that in choosing a new health-records system they would need to restart the entire OEA project? If so, what factors may have caused them to make this choice?

Sources: Neal Ungerleider, “IBM’s Watson for Business: The $1 Billion Siri Slayer,” *Fast Company*, January 8, 2014, https://www.fastcompany.com/3024604/ibms-watson-for-business-the-1-billion-siri-slayer; “MD Anderson Taps IBM Watson to Power ‘Moon Shots’ Mission,” MD Anderson, October 18, 2013, https://www.mdanderson.org/newsroom/2013/10/md-anderson–ibm-watson-work-together-to-fight-cancer.html; Mary Chris Jaklevic, “MD Anderson Cancer Center’s IBM Watson Project Fails, and So Did the Journal Related to It,” *Health News Review*, February 23, 2017, www.healthnewsreview.org/2017/02/md-anderson-cancer-centers-ibm-watson-project-fails-journalism-related/; Richard Waters, “Artificial Intelligence: Can Watson Save IBM,” *Financial Times*, January 5, 2016, https://www.ft.com/content/dced8150-b300-11e5-8358-9a82b43f6b2f; Daniela Hernandez, “Hospital Stumbles in Bid to Teach a Computer to Treat Cancer,” *Wall Street Journal*, March 8, 2017, https://www.wsj.com/articles/hospital-stumbles-in-bid-to-teach-a-computer-to-treat-cancer-1488969011; Ariana Eunjung Cha, “Why This Former Billionaire Party Boy Donated $50 Million to Try to Teach Watson to Be a Cancer Expert,” *The Washington Post*, June 26, 2015, https://www.washingtonpost.com/business/on-leadership/why-this-former-billionaire-party-boy-donated-50-million-to-transform-ibms-watson/2015/06/26/a223ee36-9c1f-11e4-bcfb-059ec7a93ddc_story.html.

2. Sophia Genetics Moves Precision Medicine Ahead

Precision medicine is an emerging approach for disease treatment that is based on recognition of each individual patient’s variability in environment, lifestyle, and genetic makeup. A particularly promising application area of precision medicine is in the treatment of patients with breast, colorectal, and lung cancers, as well as melanomas and various types of leukemia.

Individual cancer patients today receive generally the same treatment as other cancer patients with the same type and stage of cancer—based on current standard-of-care recommendations. However, different patients may respond differently to the same treatment, and, only recently, have doctors begun to understand why.

Cancer is caused by certain changes to our genes that control the way our cells grow and divide. These changes include mutations in the DNA that make up our genes. Such mutations can be inherited from our parents or acquired through exposure to certain carcinogens or the ultraviolet rays of the sun. In the ideal application of precision medicine, once physicians have identified the mutations causing a patient’s cancer, they can prescribe drugs that target and destroy only the cells associated with that mutation, as opposed to using existing chemotherapy drugs that kill all rapidly reproducing cells, whether they are cancerous or not. Patients receiving precision medicine treatments targeted specifically at cancer cells tend to experience fewer side effects, feel better, and recover more quickly.

Sophia Genetics is a Swiss-based analytics company that employs powerful artificial intelligence algorithms and a global community of hospitals to improve the treatment of patients suffering from cancer. The process begins with the extraction of the patient's DNA via a blood draw or biopsy. The hospital then prepares samples and processes them using a DNA sequencer that determines the sequence of the four chemical building blocks or nucleotides (As, Ts, Cs, and Gs) that make up an individual's DNA molecule.

The patient's DNA sequence files are uploaded to the Sophia DDM software-as-a-service platform and analyzed using patented advanced algorithms and machine learning approaches.

The software identifies variations in the patient's genetic code and then uses historical data to suggest the best combination of drugs to treat a specific cancer in an individual patient. A powerful capability of Sophia DDM is that it can compare patient data across hospitals, so its users can tell a patient that his or her cancer looks like the cancer of 1,000 other patients—of whom 600 received the recommended drug and 80 percent survived more than five years. Currently, 215 hospitals in 35 countries are using the Sophia DDM platform. The more hospitals that use the analytical platform, the more genomic profiles it analyzes, and the smarter the artificial intelligence gets.

Sophia DDM is a software-as-a-service platform, so hospitals access the service online, paying a modest fee of $50–$200 whenever they use it to enter a new sample. Healthcare professionals who use Sophia DDM for genetic sequencing and analysis can get drug treatment regime recommendations for individual patients within a day. Without this technology, the process of determining a drug treatment can take from two to several days.

The software-as-a-service approach enables smaller hospitals and clinics to afford the technology. It also allows for the democratization of information—that is, data about drug outcomes for different cancers and conditions can be used to update a database and be shared globally. Sharing the data encourages collaboration and clinics have access to experts and results from around the world.

However, precision medicine is not yet a fully developed technology and as such has limits related to cost, accuracy, and efficacy. It cannot work for all patients and all cancers. One person's tumor cells can vary depending on where in the body they are located. There can even be variation in the same tumor from the same patient. This issue of tumor heterogeneity is a key issue of precision medicine that must be addressed along with the outgrowth of cells resistant to treatment, serious adverse events, and cost. Too narrow a concentration on precision medicine may divert resources from other promising avenues of cancer research. Time is required to resolve these issues.

Critical Thinking Questions

1. What advantages does the Sophia DDM system have compared to the approach attempted by MD Anderson, as described in the previous case. Which approach do you believe has the greater potential for success in the long run? Why?
2. The creation of a patient database shared among hospitals globally raises concerns about patient privacy. How might Sophia DDM address this concern?

3. Do research to determine whether or not the Sophia DDM technology improved patient outcomes, lowered costs, or provided some other benefit. Document your findings in a brief paragraph or two.

Sources: "The Genetics of Cancer," National Cancer Institute, https://www.cancer.gov/about-cancer/causes-prevention/genetics, accessed March 1, 2017; Mary Shacklett, "How AI and Next-Generation Genomic Sequencing is Helping Cancer Patients," *TechRepublic*, February 28, 2017, www.techrepublic.com/article/how-ai-and-next-generation-genomic-sequencing-is-helping-cancer-patients/; Bérénice Magistretti, "Swiss Data Analytics Company Sophia Genetics Could Be Switzerland's Next Unicorn," *TechCrunch*, January 2, 2017, https://techcrunch.com/2017/01/02/swiss-data-analytics-company-sophia-genetics-could-be-switzerlands-next-unicorn/; Matt Burgess, "How Machine Learning is Speeding Up Cancer Diagnosis," *Wired*, May 10, 2016, www.wired.co.uk/article/sophia-genetics-sequencing-dna-cancer.

End Notes

[1] "RAND Study Says Computerizing Medical Records Could Save $81 Million Annually and Improve the Quality of Medical Care," RAND Corporation, September 14, 2005, www.rand.org/news/press/2005/09/14.html.

[2] Patrick Caldwell, "We've Spent Billions to Fix Our Medical Records, and They're Still a Mess. Here's Why," *Mother Jones*, October 21, 2015, www.motherjones.com/politics/2015/10/epic-systems-judith-faulkner-hitech-ehr-interoperability.

[3] John McQuaid, "Patient Mix-Ups Happen More Often Than You Think. Why the Easy Fix Isn't Easy at All," *STAT*, January 28, 2016, https://www.statnews.com/2016/01/28/patient-mixups-universal-identification/.

[4] Stephen L. Meigs, DHA, FACHE and Michael Solomon, PhD, MBA, "Electronic Health Record Use a Bitter Pill for Many Physicians," NLM, January 1, 2016, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4739443/.

[5] Caldwell, "We've Spent Billions to Fix Our Medical Records, and They're Still a Mess. Here's Why."

[6] Meigs and Solomon, "Electronic Health Record Use a Bitter Pill for Many Physicians."

[7] Kimberly Amadeo, "The Great Depression of 1929," *About.com*, http://useconomy.about.com/od/grossdomesticproduct/p/1929_Depression.htm.

[8] Kimberly Amadeo, "GDP 2008 Statistics," *US Economy*, April 30, 2011, http://useconomy.about.com/od/GDP-by-Year/a/2008-GDP-statistics.htm.

[9] Peter S. Goodman, "Unemployment Rate Hits 10.2%, Highest in 26 Years," *New York Times*, November 6, 2009.

[10] Shawn Sprague, "Below Trend: The U.S. Productivity Slowdown Since the Great Recession," U.S. Department of Labor Bureau of Labor Statistics, *Beyond the Numbers* 6 no. 2 (January 2017), https://www.bls.gov/opub/btn/volume-6/below-trend-the-us-productivity-slowdown-since-the-great-recession.htm.

[11] United States Department of Labor, Bureau of Labor Statistics, Labor Productivity and Costs, Productivity Change in the Nonfarm Business Sector, 1947–2010, www.bls.gov/lpc/prodybar.htm (accessed April 20, 2013).

[12] Erik Brynjolfsson and Lorin M. Hitt, "Computing Productivity: Firm-Level Evidence," November 2002, https://pdfs.semanticscholar.org/83ec/784b29a85e94a63b170f73a3a6b7851ce269.pdf.

[13] James Manyika, Michael Chui, Mehdi Miremadi, Jacques Bughin, Katy George, Paul Willmott, et al., "Harnessing Automation for a Future that Works," McKinsey Global Institute, January 2017, www.mckinsey.com/global-themes/digital-disruption/harnessing-automation-for-a-future-that-works.

[14] Andy Kessler, "The Robots Are Coming, Welcome Them," *Wall Street Journal*, August 22, 2016, https://www.wsj.com/articles/the-robots-are-coming-welcome-them-1471907751.

[15] Michael Chui, James Manyika, and Mehdi Miremadi, "Where Machines Could Replace Humans—and Where They Can't (Yet)," *McKinsey Quarterly*, July 2016, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/where-machines-could-replace-humans-and-where-they-cant-yet.

[16] *Ibid*.

[17] Jon Gertner, "IBM's Watson Is Learning Its Way to Saving Lives," *Fast Company*, October 15, 2012, https://www.fastcompany.com/3001739/ibms-watson-learning-its-way-saving-lives.

[18] "Are You Leaving Money on the Table? H&R Block with Watson Can Help," IBM, https://www.ibm.com/watson/stories/taxes.html, accessed March 20, 2017.

[19] Joseph Walker, "Alliance of Companies Unveil First Steps Aimed at Cutting Health-Care Costs," *Wall Street Journal*, March 7, 2017, https://www.wsj.com/articles/alliance-of-companies-unveil-first-steps-aimed-at-cutting-health-care-costs-1488835293.

[20] Sam Shead, "Amazon Now Has 45,000 Robots in Its Warehouses," *Business Insider*, January 3, 2017, www.businessinsider.com/amazons-robot-army-has-grown-by-50-2017-1.

[21] Aaron Smith and Janna Anderson, "Predictions for the State of AI and Robotics in 2025," Pew Research Center, August 6, 2014, www.pewinternet.org/2014/08/06/predictions-for-the-state-of-ai-and-robotics-in-2025.

[22] "How Can We Teach Morals to Robots? By Telling Them Stories," *Popular Science*, February 17, 2016, www.popsci.com/how-to-teach-morals-to-robots-by-telling-stories.

[23] Benjamin Mullin, "Robot-Writing Increased AP's Earnings Stories by Tenfold," *Poynter*, January 29, 2015, https://www.poynter.org/2015/robot-writing-increased-aps-earnings-stories-by-tenfold/315931/.

[24] Kimberly Amadeo, "The Rising Cost of Health Care and Its Causes," *The Balance*, January 20, 2017, https://www.thebalance.com/causes-of-rising-healthcare-costs-4064878.

[25] "National Health Expenditure Projections 2016–2025," Centers for Medicare & Medicaid Services, https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/proj2016.pdf, accessed February 27, 2017.

[26] Louis Goodman and Timothy Norbeck, "Who's to Blame for Our Rising Healthcare Costs?" *Forbes*, April 3, 2013, www.forbes.com/sites/realspin/2013/04/03/whos-to-blame-for-our-rising-healthcare-costs.

[27] "Dr. Reed Uses Health IT to Help Her Patients Improve Health and Wellness," HealthIT.gov, https://www.healthit.gov/providers-professionals/dr-reed-uses-health-it-help-her-patients-improve-health-and-wellness (accessed March 11, 2017).

[28] “Dr. Carpio Optimizes EHR System to Eliminate Gaps in Care,” HealthIT.gov, https://www.healthit.gov/providers-professionals/dr-carpio-optimizes-ehr-system-eliminate-gaps-care (accessed March 11, 2017).

[29] “Published Costs of Medication Errors Leading to Preventable Adverse Drug Events in US Hospitals,” ISPOR 20th Annual Meeting, Philadelphia, May 18–20, 2015, https://www.ispor.org/research_pdfs/49/pdffiles/PHP73.pdf.

[30] Teryl K. Nuckols, Crystal Smith-Spangler, Sally C. Morton, Steven M. Asch, Vaspaan M. Patel, Laura J. Anderson, et al., “The Effectiveness of Computerized Order Entry at Reducing Preventable Adverse Drug Events and Medication Errors in Hospital Settings: A Systematic Review and Meta-Analysis,” *Systemic Reviews*, 2014, https://systematicreviewsjournal.biomedcentral.com/articles/10.1186/2046-4053-3-56.

[31] Lori Roniger, “Telemedicine Is Convenient…But More Importantly It Saves Money,” *Healthline*, July 18, 2016, www.healthline.com/health-news/telemedicine-convenient-saves-money.

[32] Jacquelyn Corley, MD, “Telemedicine Is Saving Lives in Rural America and Around the World,” *The Hill*, March 7, 2016, http://thehill.com/blogs/congress-blog/healthcare/271818-telemedicine-is-saving-lives-in-rural-america-and-around-the.

[33] “James Spillane Uses Health IT to Improve Care Coordination in a Remote Region of Alaska,” HealthIT.gov, https://www.healthit.gov/providers-professionals/james-spillane-uses-health-it-improve-care-coordination-remote-region-alaska, accessed March 11, 2017.

[34] Justin Montgomery, “mHealth: iPhones to Provide Mobile Means for Monitoring Blood Pressure,” *mHealthWatch*, June 11, 2011, http://mhealthwatch.com/mhealth-iphones-to-provide-mobile-means-for-monitoring-blood-pressure-16425.

[35] Justin Montgomery, “JCAHO Issues Ban on Physician Texting, Signifies Importance of Secure Mobile Communication Outside SMS,” *mHealthWatch*, November 29, 2011, http://mhealthwatch.com/jcaho-issues-ban-on-physician-texting-signifies-importance-of-secure-mobile-communication-outside-sms-18266.

[36] Matthew Wall, “The Proven Health Trackers Saving Thousands of Lives,” *BBC*, November 15, 2016, www.bbc.com/news/business-37972606.

[37] Pauline W. Chen, MD, “Are Doctors Ready for Virtual Visits,” *New York Times*, January 7, 2010, www.nytimes.com/2010/01/07/health/07chen.html.

CHAPTER 9

SOCIAL MEDIA

QUOTE

> *Regarding social media, I really don't understand what appears to be the general population's lack of concern over privacy issues in publicizing their entire lives on the Internet for others to see to such an extent … but hey it's them, not me, so whatever.*
>
> —Axl Rose, lead vocalist for Guns N' Roses

Luba V Nel/Shutterstock.com

ORGANIZATIONS BEHAVING BADLY

With over 1.8 billion monthly active users, Facebook is obviously providing a service that an awful lot of people want. It is a marvelous way to stay connected with friends and family, find out what's going on in the world, identify and develop new business contacts, and share thoughts and feelings that are important to you. In addition to individual users, millions of companies maintain Facebook pages to advertise their goods and services, improve relationships with both current and potential customers, and communicate their viewpoint on important issues of the day. But there is also a dark side to

Facebook: some people use it as a stage on which to perform at their very worst. Some of the most damaging behavior on Facebook (and other social networking platforms), include the following:

- Careless users post rumors, gossip, and half-truths without stopping to consider how quickly their words will spread, potentially negatively affecting others.
- Cyberbullies harass, torment, humiliate, and threaten others—making their victim's lives miserable, even driving some to commit suicide.
- Pseudo-journalists post fake news stories for profit or to support their cause.
- Deeply disturbed individuals live-stream their own suicide.
- Cyberstalkers threaten or make unwanted advances toward others putting them in fear of their life.
- Demented individuals live-stream themselves committing atrocities and violent crimes.

What responsibility do the users of a social network have to not harm others? What can Facebook and operators of other social networks do to reduce the number of bad actors who use their service? What should they do?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. How do individuals use social networks, and what are some practical business uses of social networking and other social media tools?
2. What are some of the key ethical issues associated with the use of social networks and other social media?

WHAT IS SOCIAL MEDIA?

Social media are web-based communication channels and tools that enable people to interact with each other by creating online communities where they can share information, ideas, messages, and other content, including images, audio, and video. Common features of social media are user accounts, profile pages (for individuals, groups, and businesses), friends or followers, event pages, news feeds, media-sharing features, like buttons, comments sections, and reviews—among others. Different types of social media are blogs (with comments sections), discussion forums, media-sharing networks, wikis, social bookmarking tools, social messaging apps, and social networking, news, and shopping platforms.[1] Often (including throughout this chapter), the term *social networking* is used interchangeably with the term *social media* to describe the apps, websites, and other tools that allows users to interact online.

SOCIAL NETWORKING PLATFORMS

A **social networking platform** creates an online community of Internet users that enables members to break down barriers created by time, distance, and cultural differences. Social networking platforms allow people to interact with others online by sharing opinions, insights, information, interests, and experiences. Some platforms, such as LinkedIn, are more text focused. Others, such as Instagram, Snapchat, Tumblr, and YouTube, are primarily focused on audio and visual content. Members of an online social network may use the platform to interact with friends, family members, and colleagues—people they already know—but they may also make use of the platform to develop new personal and professional relationships.

With the number of Internet users worldwide approaching 4 billion (just under 50 percent of the world population), there is an endless range of interests represented online, and a correspondingly wide range of social networking platforms catering to those interests.[2] Some platforms cater to a specific—and sometimes narrow—audience, while others, such as Facebook and Twitter, allow users to explore a range of interests by following friends, public figures, media organizations, specific brands, and sports teams all via one platform. Table 9-1 lists some of the most popular social media platforms, based on the number of unique visitors per month.

TABLE 9-1 Popular social networking platforms

Social networking platform	Unique monthly visitors (million)
Facebook	1,100
YouTube	1,000
Twitter	310
LinkedIn	255
Pinterest	250
Google Plus+	120
Tumblr	110
Instagram	100
Reddit	85
VK	80
Flickr	65
Vine	42
Meetup	40
Ask.fm	37
ClassMates	15

Source: “Top 15 Most Popular Social Networking Sites|March 2017,” ebizmba, www.ebizmba.com/articles/social-networking-websites.

According to Nielsen, the global information and measurement company, Generation Xers (born 1965 to 1980) spend the most time on social media (almost 7 hours per week), while Millennials (born 1981 to 1997) spend just over 6 hours per week using social media. Women spend more time using social media than men—6 hours and 33 minutes per week on average compared to 4 hours and 23 minutes per week for men.[3] Of course, the social media phenomenon is not limited to the United States. Around the world, the increasing availability of mobile networks has brought a corresponding increase in the use of social media on mobile devices. Figure 9-1 provides a look at the global mobile social network penetration rate (percent of total population that uses social media on a mobile device) by region.

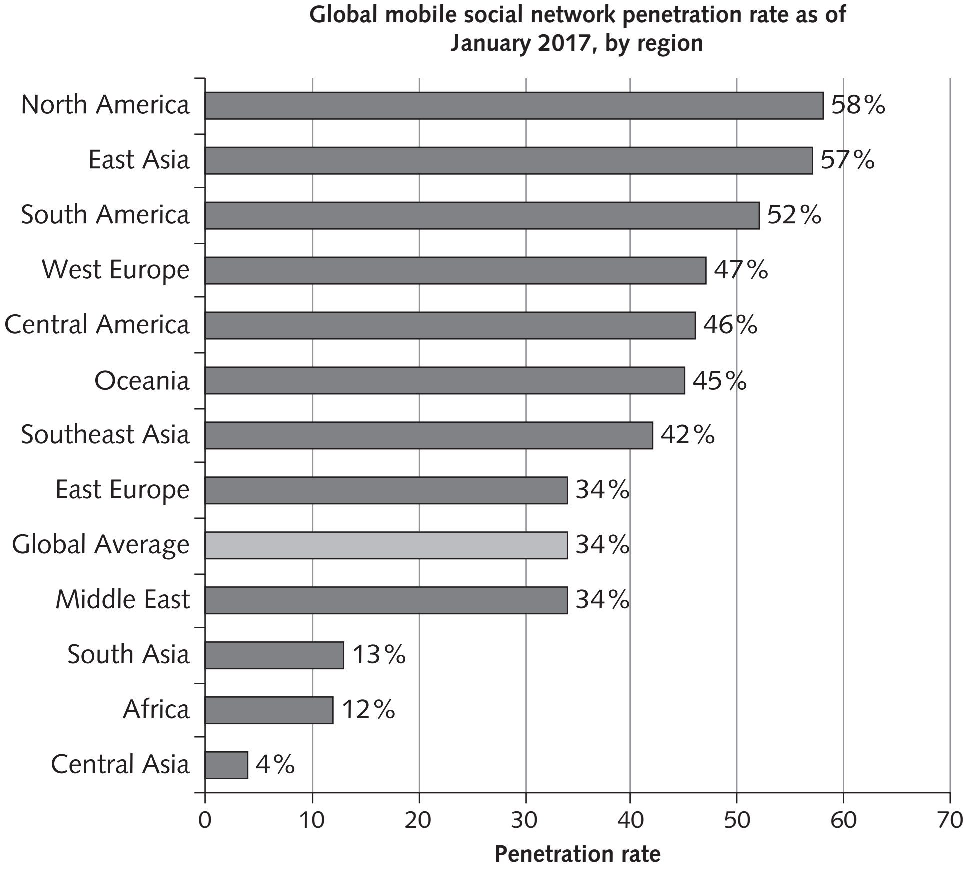


FIGURE 9-1 Global mobile social network penetration rate, as of January 2017

Source: Global mobile social network penetration rate as of January 2017, by region at https://www.statista.com/statistics/412257/mobile-social-penetration-rate-region/

BUSINESS APPLICATIONS OF SOCIAL MEDIA

Although many social networking platforms were originally targeted at nonbusiness users, many organizations now use social media tools to advertise, assess job candidates, and sell products and services. An increasing number of business-oriented social networking platforms including Facebook, LinkedIn, Instagram, Twitter, Google/YouTube, and Yelp can be used to encourage and support relationships with consumers, clients, potential employees, suppliers, and business partners around the world.

With over 1.1 billion unique visitors each month, Facebook includes the largest blend of demographics of all the social networks. It is a massive social media platform that provides online marketing tools that make it easier for organizations to develop marketing campaigns and reach their target audience; a first step in using Facebook is to develop a Facebook page that allows customers to "Like" the page and post their comments and reviews about the company's products and services. Organizations can use Facebook as a platform to promote and inform customers about their latest initiatives and promotions.

Companies can use LinkedIn, the world's largest professional network, to develop contacts with clients, promote themselves, and connect with individuals and organizations within their industry. It can also be used to find highly skilled employees and contractors. LinkedIn Groups enables organizations to create groups to target a particular industry niche, and then invite LinkedIn members in the target group to join.

Attendees of organization events and tradeshows can be encouraged to post photos to the popular photo-sharing platform Instagram to create more buzz about their company or event.

Twitter enables an organization to share short text updates, images, links, polls, and videos. Hashtags, which can be used to quickly spread a company's message, allow a company's tweets to be seen not only by its followers but also by those who are interested in the topic being tweeted about. For instance, a hashtag with a product name allows anyone interested in the product to see the tweet regardless of whether they are following the company.

Organizations can use Google Hangouts On Air to capture interviews with customers, managers, and industry leaders. The interviews are then posted automatically to YouTube under the company's account to provide greater visibility.

Organizations need a strategy to build positive reviews on Yelp and prevent any negative review from drawing attention. Without such a strategy, any negative comment can stand out and detract from the rating of your business. Many organizations carefully monitor their presence on social media to avoid such problems.

There are new social networking platforms springing up all the time. Table 9-2 lists additional platforms of interest.

TABLE 9-2 Other popular business-oriented social media platforms

Platform	Description of how used
DoMyStuff	A social marketplace designed to connect people who want stuff done with people who will do it; it enables users to outsource business tasks to thousands of assistants bidding on the jobs—an alternative to hiring a temp agency to fill short-term needs.
IndustryHuddle	An online community of suppliers, distributors, and customers networking in their industries for B2B online sales; it promises to help companies connect with manufacturers and customers in their industries, increase product sales, and grow their business networks.
GoBigNetwork	An online community that helps connect companies with investors over 300,000 start-ups have used this community to find funding.
PartnerUp	An online networking community used by entrepreneurs and small business owners to find the expertise and resources they need to start and grow a business; members can connect with potential partners, advisers, and business resources.

Social Media Marketing

Social media marketing involves the use of social networks to communicate and promote the benefits of products and services. According to Nielsen, about 37 percent of all consumers say they use social media to find out about products and services, while about 32 percent use social media to receive exclusive offers, coupons, or other discounts from brands.[4]

The two primary objectives of social media marketers are raising brand awareness and driving traffic to a website to increase product sales. Other important benefits of social media marketing are developing loyal fans, providing market insight, and generating leads.

Two significant advantages of social networking marketing over more traditional media—such as radio, TV, and newspapers—are that marketers can create an opportunity to generate a conversation with viewers of the message, and those messages can be targeted to reach people with the desired demographic characteristics.

The overwhelming majority of social media marketers use Facebook ads (87%), Google ads (39%), Twitter ads (19%), and LinkedIn ads (17%) are the next most popular. Organizations may employ one or more social media marketing strategies including organic, paid, and earned social media marketing.

Organic media marketing employs tools provided by or tailored for a particular social media platform to build a social community and interact with it by sharing posts and responding to customer comments on the organization's blog and social media accounts. Social networks do not charge for organic media marketing. Organizations may elect to pay to use a third-party app, such as Hootsuite, to manage and schedule posts to multiple social media profiles on Facebook, LinkedIn, Instagram, and Twitter. Many social media networks use algorithms designed to deliver the most relevant content to each individual user. On most platforms, however, these algorithms give preference to posts from family and friends, making it more difficult for an organization to get its message through. As a result, organic media marketing is on the decline.

Paid media marketing involves paying a third party to broadcast an organization's display ads or sponsored messages to social media users. An organization can acquire paid social media traffic through social media ads on Facebook, LinkedIn, Twitter, YouTube, and many other social media marketing channels. Paid media marketing enables an organization to target a specific audience—based on demographics and other factors—to increase the percentage of their target audience that is exposed to its content. Thus, an ad for a new magazine on mountain biking could be directed to individuals on a social networking platform who are male, who are between 18 and 35 years old, and who express an interest in mountain biking. Others on the social network would not see the ad.

Two common methods of charging for paid media are cost per thousand impressions and cost per click. **Cost per thousand impressions (CPM)** ads are billed at a flat rate per 1,000 impressions, which is a measure of the number of times an ad is displayed—whether it was actually clicked on or not. There is no additional charge for any clicks that the ad receives. **Cost per click (CPC)** ads are paid for only when someone actually clicks on them.

Earned media refers to the media exposure an organization gets through press and social media mentions, positive online ratings, and reviews, tweets and retweets, reposts (or "shares"), recommendations, and so on. Earned social media traffic enables an organization to reach more people without any additional cost. The volume of earned media is also a factor in determining how high an organization ranks in Google's search engine.

Global social media marketing spending nearly doubled from 2014 to 2016, increasing from $16 billion to $31 billion—or 6.4 percent of total global advertising spending of $480 billion. Social media ad spending in the United States alone is expected to increase to $17 billion in 2019.[5,6]

In its ongoing fight for market share in the beverage industry, Coca-Cola has implemented a number of social networking initiatives to promote its brands:

- Visitors to the company's "Our Company" page on its main corporate website will access a new site titled, *Coca-Cola Journey*, which provides information about Coca-Cola brands and history, collectibles, advertising, and the brand's role in pop culture.
- The Coca-Cola Facebook page includes fans' stories and posts from company workers showing how people from around the world have helped make Coke into what it is today. The page is monitored by software filters for offensive words and phrases, and live moderators check its pages for anything truly offensive, while also responding to users' comments, compliments, and complaints. The company generally lets Facebook fans say what they want on the page, which currently boasts over 104 million followers.
- The company strongly encourages its 150,000 associates to share brand messages on their own social media accounts.[7]

Surprisingly, Coca-Cola executives admit that it is hard to find a direct link between online buzz (social chatter) and short-term sales. However, the company strongly believes that social media is an essential component of its overall marketing program.[8]

Viral marketing is an approach to social media marketing that encourages individuals to pass along a marketing message to others, thus creating the potential for exponential growth in the message's exposure and influence as one person tells two people, each of those two people tell two or three more people, and so on. The goal of a viral marketing campaign is to create a buzz about a product or idea that spreads wide and fast.

California-based Vans, a shoe and apparel company, achieved viral success thanks to two teenagers and their running Snapchat joke, "Damn Daniel." The catchphrase was used in a video medley featuring a voiceover of a teenager complimenting his friend Daniel on his fashionable attire, which included Vans shoes, on several different occasions. Vans experienced an instant spike in sales, with a 20 percent increase in direct-to-consumer sales and a 30 percent rise in online sales.[9]

Social Media in the Hiring Process

According to CareerBuilder, 60 percent of employers used social media to research job candidates in 2016. Nearly half of those companies found information on social media that gave a negative impression of the candidate. The offending content included inappropriate photographs and videos, information about the candidate drinking or using drugs, and discriminatory comments related to gender, race, and religion.[10]

Social media users frequently provide sex, age, marital status, sexual orientation, religion, and political affiliation data in their profiles. Users who upload personal photos may reveal a disability or their race or ethnicity; therefore, without even thinking about it, an individual may have revealed data about personal characteristics that are protected by civil rights legislation. Employers can legally reject a job applicant based on the individual's social media activity only if the company is not violating federal or state discrimination laws. For example, an employer cannot legally screen applicants based on race or ethnicity. Or suppose that by checking a social networking site, a hiring manager finds out that a job candidate is pregnant and makes a decision not to hire that person based on that information. That employer would be at risk of a job employment discrimination lawsuit because refusing to hire on the basis of pregnancy is prohibited by the Pregnancy Discrimination Act, which amended Title VII of the Civil Rights Act of 1964.

Job seeking candidates should review their presence on social media and remove photos and postings that portray them in a potentially negative light. Many jobseekers delete their social media accounts altogether because they know employers check such sites. Jobseekers must realize that pictures and words posted online, once intended for friends only, can reach a much larger audience and can have an impact on their job search.

Improving Customer Service Using Social Media

In the past, companies relied heavily on their market research and customer service organizations to provide them with insights into what customers think about their products and services. For example, many consumer goods companies put toll-free 800 numbers on their products so that consumers could call in and speak with trained customer service reps to share their comments and complaints. Increasingly, however, consumers are using social networks to share their experiences, both good and bad, with others. And the old adage "A happy customer tells a few people, an unhappy customer tells everyone" has never been more true.

Customers also use social media to seek advice on how to use products more effectively and how to deal with special situations encountered when using a product. Global market research company J.D. Power claims that two-thirds of consumers have used a company's social media channel for customer service. Many of these consumers have very high expectations: 42 percent feel they should receive a response with an hour.[11]

Unless organizations actively monitor and engage with customers on social media, their customers may be left to resolve their issues and questions on their own, often in ways that are not ideal. The end result can be dissatisfaction with the product and loss of customers and future sales. Thus, progressive companies are focusing more resources on monitoring issues and assisting customers via social media. One of the major challenges with these efforts is in filtering the few nuggets of actionable data from the volumes of chatter and converting these key findings into useful business actions.

A few years ago, General Motors created a Social Media Center of Expertise (CoE) staffed by 600 people whose goal is to enhance the company's market-based decision making. In North America, 26 full-time social media customer care advisers monitor 150 social media channels owned by GM and its Buick, Cadillac, Chevrolet, and GM divisions. The customer care advisers also cover another 85 or so websites where GM is likely to be mentioned—such as auto enthusiast blogs and forums. Through this program, GM became aware of a faulty climate-control component in its vehicles when a customer posted comments to a product-owner blog. The CoE worked with engineers at GM to find the root cause of the problem. The company then issued a technical service bulletin instructing all GM dealerships to replace the defective component on all cars in their inventory. GM also made changes in production so that no new auto would be affected by the problem. The original poster, who never asked GM directly for help, had his vehicle fixed within 10 days of his original posting.[12]

Social Shopping Platforms

Social shopping platforms combine two highly popular online activities—shopping and social networking. Their growth in popularity can be attributed to two things: choice overload and users eager for expert advice to decide what to purchase. Members of social shopping sites can typically build their own pages to collect information and photos about items in which they are interested. Some social shopping platforms have implemented a reward system for members, in which they are paid a commission each time another shopper acts on their recommendation to purchase a specific item.[13] There are numerous social shopping platforms, a few of which are summarized in Table 9-3.

TABLE 9-3 Sample of social shopping platforms

Platform	Description
Fancy	A site where users can discover products that have been curated by its global community and buy from thousands of different stores directly through the platform; each user gets their own profile that shows off everything that they "Fancy'd." By following others members, users can see the products those users are Fancying in their feed.
MyDeco	A site with a focus on interior design and home decor; users can mock up virtual rooms using their favorite products.
MyITThings	Both a shopping site and a fashion magazine that allows users to place products they bought in a virtual closet; the platform also allows users to review books, music, and other products.
OpenSky	A platform that offers products for sale in a wide variety of categories, including accessories, beauty, clothing, electronics, jewelry, kitchen, sporting goods, toys, and more; users can add products to their wish lists, follow other sellers, and invite friends to join in order to earn shopping rewards, such as shipping deals and credits toward future purchases.
Pinterest	One of the most popular social shopping sites and visual bookmarking tools; Pinterest enables users to visually share and discover new interests (recipes, parenting tips, style ideas, etc.) by posting (known as "pinning") images or videos to their own or others' boards. Users can also browse items that other users have pinned.

(*continued*)

TABLE 9-3 Sample of social shopping platforms (*Continued*)

Platform	Description
Polyvore	A combination social network and digital fashion magazine popular with home designers and clothing fashionistas, who can use its tools for grouping related items visually; users find images of things they like all from sites across the web, and then save them into sets of related images, which the site calls collages.
Wanelo	An Internet shopping mall where people can discover and make purchases from a broad selection of over 12 million products; the more that you interact on Wanelo and the more products that you save, the more the site learns about you and the better it's able to recommend products based on what you already like.

Social shopping platforms generate revenue through retailer advertising. Retailers can purchase member data and comments via some social shopping platforms to find out what consumers like and don't like and what they are looking for in items sold by the retailer. This can help the retailer design product improvements and come up with ideas for new product lines.

CRITICAL THINKING EXERCISE

Your organization specializes in selling fashionable clothes to tweens (age 10 to 12) who wear only the most carefully selected clothes that allow them to project the exact image they want to put out there, right down to their socks. The head of marketing for your company wants to augment in-store sales with sales from a social shopping platform. How might such a platform be designed to appeal to the target audience? What special issues might arise in marketing to this youthful market?

SOCIAL NETWORKING ETHICAL ISSUES

When you have an Internet community of nearly 4 billion people online, not everyone is going to be a good "neighbor" and abide by the rules of the community. Many will stretch or exceed the bounds of generally accepted behavior. Some common ethical issues that arise for members of social networking platforms are online abuse, harassment, stalking, cyberbullying, encounters with sexual predators, the uploading of inappropriate material, and the participation of employees in social networking. Additional social networking issues include the increased risk of accidents associated with social media interaction while driving, the tendency of many social media users to become narcissist in their postings, and the ability to perform self-image manipulation.

Cyberabuse, Cyberharassment, and Cyberstalking

Cyberabuse is any form of mistreatment or lack of care, both physical and mental, based on the use of an electronic communications device that causes harm and distress to others. Cyberabuse encompasses both cyberharassment and cyberstalking, a broad spectrum of behaviors wherein someone acts in a way that causes harm and distress to others. Instances of cyberabuse are not always clear. **Cyberharassment** is a form of cyberabuse in which the abusive behavior, which involves the use of an electronic communications device, is degrading, humiliating, hurtful, insulting, intimidating, malicious, or otherwise offensive to an individual or group of individuals causing substantial emotional distress. Nearly three-quarters (72 percent) of U.S. Internet users have witnessed online harassment or abuse, and almost half (47 percent) have personally experienced cyberabuse.[14]

Here are a few tips to help you avoid becoming a victim of cyberabuse:

- Always use a strong, unique password (12-plus characters, including a mix of numbers, capital letters, and special characters) for each social networking site.
- If you broke up with an intimate partner, reset the passwords on all of your accounts, including email, financial, and social networking accounts.
- Check your privacy settings to ensure that you are sharing only the information you want to share with only people you trust and not the general Internet public.
- Some sites have options for you to test how your profile is being viewed by others—use this feature to make sure you only reveal what is absolutely necessary.
- Warn your friends and acquaintances not to post personal information about you, especially your contact information and location.
- Don’t post photographs of your home that might indicate its location by showing the street address or a nearby identifying landmark.
- If you connect your smartphone to your online account, do not provide live updates on your location or activities.
- Avoid posting information about your current or future locations.
- Do not accept “friend requests” from strangers.
- Avoid online polls, quizzes, or surveys that ask for personal information.

Cyberstalking is a subcategory of cyberabuse that consists of a long-term pattern of unwanted, persistent pursuit and intrusive behavior (involving the use of an electronic communications device) that is directed by one person against another and that causes fear and distress in the victim. Occasionally, cyberstalkers are complete strangers, but it is more common for victims to know the stalker. Cyberstalking can be a serious problem for victims, terrifying them and causing mental anguish. It is not unusual for cyberstalking to escalate into abusive or excessive phone calls, threatening or obscene mail, trespassing, vandalism, physical stalking, and even physical assault. Overall, 8 percent of U.S. Internet users say they have experienced cyberstalking to the point of feeling unsafe or afraid. Young people, especially women under 30, are more likely to be targets of cyberstalking. It is estimated that 14 percent of Internet users under 30 year of age have been cyberstalked, including 20 percent of women under 30.[15]

Note that cyberharassment differs from cyberstalking in that it is aimed at tormenting an individual but does not involve a credible threat of physical harm.[16] Table 9-4 provides examples of cyberharassment and cyberstalking.

TABLE 9-4 Examples of cyberharassment and cyberstalking

Cyberharassment	Cyberstalking	Neither
Someone keeps sending you instant messages after you have asked them to stop.	Someone sends you a credible threat that they are "out to get you."	Someone posts a strongly worded dissenting opinion to your post on a social network.
Someone posts a message in such a manner that it appears to have come from you.	An unknown individual keeps sending you messages like, "I saw you at….": the messages name specific locations you have been.	Someone posts a message disparaging members of a particular race, ethnic group, or sexual orientation to which you belong.
Someone posts explicit or embarrassing photos or videos of you (revenge porn) without your permission.	An unknown individual posts photos of you taken over several days in different locations, without you even being aware that your photo was taken.	

The National Center for Victims of Crime offers a detailed set of recommended actions to combat cyberstalking, including the following:

- Contact local law enforcement authorities to obtain a restraining order prohibiting any further contact with you.
- Inform your ISP provider as well as the stalker's ISP.
- Provide the stalker a written notice that their contact is unwanted and that all further contact must cease.
- Consider suspending your social networking accounts until the cyberstalking situation has been resolved.
- Gather as much physical evidence as possible and document each instance of abusive contact.
- Never agree to meet with the stalker to "talk things out."

Additional information regarding cyberabuse is available at the sources listed in Table 9-5.

TABLE 9-5 Resources for information related to cyberabuse

Organization	Website
Association for Progressive Communications	https://www.apc.org/en/pubs/issue/how-avoid-becoming-cyberstalking-victim
FightCyberstalking	https://www.fightcyberstalking.org
Privacy Rights Clearinghouse	https://www.privacyrights.org
Working to Halt Online Abuse	http://www.haltabuse.org
Stalking Risk Profile	https://www.stalkingriskprofile.com/victim-support/cyberstalking

All 50 states have anti-stalking laws, and most of those laws address cyberstalking. In some states, to qualify as a stalker, the perpetrator must make a credible threat of violence against the victim. Other states require only that the perpetrator's conduct constitute an implied threat.[17] There are also federal laws that address cyberstalking as shown in Table 9-6.[18]

TABLE 9-6 Federal laws addressing cyberstalking

Federal law	Scope
18 USC §2425	Protects children against online stalking by making it a federal crime to communicate with any person with the intent to solicit or entice a child into unlawful sexual activity.
18 USC §2261A	Makes it a federal crime for any person to travel across state lines with the intent to injure or harass another person.
47 USC §223	Makes it a federal crime to use a telephone or telecommunications device to annoy, abuse, harass, or threaten any person at the called number.
18 USC §875(c)	Makes it a federal crime to transmit any communication in interstate or foreign commerce containing a threat to injure another person.

Depending on the jurisdiction, a misdemeanor cyberstalking sentence may result in a prison sentence of up to a year in a county jail and fines of up to $1,000. Certain circumstances (for example, the accused trespassed or already has multiple cyberstalking charges or the victim was under 18 years of age) can raise a cyberstalking charge to a fourth-degree felony. A felony cyberstalking sentence may result in up to five years in a state prison, fines of up to $1,000, and possible lifetime registration as a sex offender. Both misdemeanor and felony cyberstalking convictions may subject the perpetrator to counseling, possible confinement in a state-run hospital that treats mental illness, and a restraining order prohibiting any contact with the alleged victim.

Encounters with Sexual Predators

Some social networking platforms, law enforcement, and the courts have been criticized for not doing enough to protect minors from encounters with sexual predators. Most law enforcement officers understand that dangers exist in not mandating Internet restrictions for repeat sex offenders but also realize that creating a national policy would be difficult because even convicted felons have first amendment rights. A federal court ruled in early 2013 that an Indiana state law that prohibited use of social networks by registered sex offenders violated the First Amendment rights of the sex offenders and was unconstitutional. Similar laws in Nebraska and Louisiana have also been ruled unconstitutional. Eight other states have enacted laws that in some way restrict the use of the Internet by sex offenders.[19]

The 1994 Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act set the initial requirements for sex offender registration and notification in the United States. The act requires sex offenders to register their residence with local law enforcement agencies. It also required that states create websites that provide information on sex offenders within the state. The goal of the act was to provide law enforcement and citizens with the location of all sex offenders in the community. However, which sex offenders and what data would appear on the websites was left to the various states to decide. Because of the lack of consistency among the various states, the act was less effective than desired, and sex offenders sometimes simply moved to states with less strict reporting requirements to avoid registering.[20] The act was named after an 11-year-old Minnesota boy who was abducted and murdered in 1989.

The Sex Offender Registration and Notification Provisions (SORNA) of the Adam Walsh Child Protection and Safety Act of 2006 improved on the Wetterling Act by setting national standards that govern which sex offenders must register and what data must be captured, as shown in Table 9-7.[21]

TABLE 9-7 Sex offender SORNA data requirements

Data provided by the sex offender	Data provided by jurisdiction in which the offender is registered
• Name • Social Security number • Residence address • Name and address of place of employment • Name and address of any school attending • License plate and description of any auto owned or operated by the offender	• Physical description of the sex offender • Text defining the sex crime for which the offender is registered • Criminal history of the offender including the date of all arrests and convictions • A current photo of the offender • A copy of the driver's license or photo ID issued to the offender by the jurisdiction • A set of fingerprints and palm prints • A DNA sample

The Adam Walsh Act also defines three tiers of sex offenders, each with different length of registration times and verification frequencies as shown in Table 9-8.[22] The act was named for Adam Walsh, a young boy abducted from a Florida shopping mall and later found murdered.

TABLE 9-8 Registration times and verification frequencies

Sex offender tier	Length of time sex offender must remain registered	In-person verification of sex offender data required
3	Lifetime	Every 3 months
2	25 years	Every 6 months
1	15 years	Each year

Although the deadline for implementing a comprehensive national system for the registration of sex offenders was originally July 2009, none of the jurisdictions (the 50 states, five U.S. territories, the District of Columbia, and certain Indian tribes) met this goal. As a result, the Department of Justice granted two separate one-year extensions. However, as of March 2017, only 17 states had implemented the SORNA requirements of the Adam Walsh Act.[23] Law enforcement agencies point out that their workload has increased due to the increased frequency that offenders must update their registration data. In addition, public defenders and probation officers state that SORNA has made it more difficult for sex offenders to find housing and employment, thus making it more difficult for offenders to reintegrate into the community.[24]

Uploading of Inappropriate Material

Most social networking platforms have terms of use agreements, a privacy policy, or a content code of conduct that summarizes key legal aspects regarding use of the site. Typically, the terms state that the site has the right to delete the material and terminate user accounts that violate the site's policies. The policies set specific limits on content that is sexually explicit, defamatory, hateful, violent, or that promotes illegal activity.

Policies do not stop all members of the community from attempting to post inappropriate material, and Section 230 of the Communications Decency Act protects a website from certain liabilities resulting from the publication of objectionable materials posted by the users of that website. Most sites do not have sufficient resources to review all materials submitted for posting. For example, more than 400 hours of content are uploaded to YouTube every minute. Quite often, it is only after other members of a social networking site complain about objectionable material that such material is taken down. This can be days or even weeks.

Inappropriate material posted online includes nonconsensual posts that comprise intimate photos or videos of people without their permission; such posts are often referred to as "revenge porn." This type of content is often uploaded by ex-partners with an intention to shame, embarrass, and/or harass their former partner. Revenge porn content is sometimes linked to the person's other online accounts, such as Facebook, LinkedIn, or even an employer's website, along with personal information including addresses and telephone numbers. In this context, revenge porn can be considered a form of domestic abuse and stalking.

In March 2017, a report revealed that more than 2,500 photos of female Marines in various stages of undress or engaging in sexual acts had been posted to a closed Facebook group (called Marines United) with more than 30,000 members.[25] One month after discovery of the material, Facebook announced that it would modify its procedures for dealing with such material. In the future, when such content is reported to Facebook, a trained member of its community standards team will review it. If deemed in violation of the terms of the user agreement, the content will be removed and the account of the individual who posted it will be disabled. Facebook will employ artificial intelligence and image recognition to identify and prevent the posting of similar images in Facebook, Messenger, and Instagram.[26]

Employee Participation on Social Media Networks

The First Amendment of the U.S. Constitution protects the right of freedom of expression from *government* interference; however, it does not prohibit free speech interference by *private employers.* So, while state and federal government employees have protection from retaliation for exercising certain First Amendment rights, some 18 percent of private employers surveyed say they have dismissed employees because of something they posted on social media.[27]

In 2016, a woman posted an expletive-laden, racist rant on her personal Facebook page. After another Facebook user checked her Facebook profile and discovered that she was a Bank of America employee, the bank received thousands of phone calls and social media comments challenging the hateful post. Her managers learned of the post one day, investigated, and fired her the next day for her inexcusable comments.[28]

Organizations should put in place a social media policy to avoid legal issues and set clear guidelines and expectations for employees. With a policy in place, employees can feel empowered to exercise creativity and express their opinions without concern that what they are sharing on social media could negatively impact their career.[29] Many examples of an effective employee social media policy that can be customized to meet your company's specific needs can be found online.[30] Table 9-9 provides a checklist for reviewing your organization's social media policy. The preferred answer to each question is *yes*.

TABLE 9-9 Manager's checklist for an effective social media policy

Question	Yes	No
Does it require employees to have an "opinions are my own" disclaimer on their social media profiles?		
Does it require that employees be transparent and state that they work at (COMPANY)?		
Does it provide advice on overall conduct such as "act respectfully," or "be part of the solution, not part of the problem?"		
Does it address the need to maintain confidentiality on unannounced product releases, company financial data, and nonpublic company news?		
Does it provide guidance on posting about the competition—for example, "be sure to behave diplomatically, have the facts straight, and obtain appropriate permissions?"		
Does it provide guidance on branding (what customers can expect from your product and how it is different from the competition) and how to talk about specific products?		
Does it provide advice on how employees should react if they see negative content regarding your brand?		
Does it remind employees that they should credit original sources if they are reposting or posting copyrighted material?		
Does it offer practical advice on how to respond to complaints respectfully and tactfully?		
Does it address the need to protect the personal privacy of both customers and employees?		
Does it clearly state that disciplinary action leading up to and including termination will be taken if employees do not follow this policy's guidelines?		

Miscellaneous Social Media Issues

Although many drivers believe that talking on a phone does not affect their driving, studies found that this activity quadruples your risk of an accident to about the same level as if you were driving drunk! That risk doubles again, to eight times normal, if you are texting.[31]

Social media brings out the narcissist tendencies of users driving them to go on and on about how great their life is and all the wonderful things they are doing. Such postings paint an unrealistic picture of the individual and become tedious to many while others may become discouraged that their lives are not as interesting.

Social media platforms also enable a degree of self-image manipulation. For example, Snapchat provides filters that alter the user's face by smoothing and whitening skin, changing eye shape, nose size, and jaw profile. Some users favor the filters because they enable users to feel more confident posting their photo while others feel that the filters promote an unrealistic and Westernized standard of beauty.[32]

CRITICAL THINKING EXERCISE

The vice president of marketing at your company wants to start a program to encourage employees to share messages about the organization, its products, and its services on their own social media accounts. The goal is to expand awareness of the company and to create a more positive perception. What might be the advantages of such a program? What potential issues might arise? What sort of guidelines should employees be given about what they should and should not post? Should employees be offered an incentive to participate?

Summary

How do individuals use social networks, and what are some practical business uses of social networking and other social media tools?

- Social media are web-based communication channels and tools that enable people to interact with each other by creating online communities where they can share information, ideas, messages, and other content, including images, audio, and video.
- A social networking platform creates an online community of Internet users that enables members to break down barriers created by time, distance, and cultural differences; such a site allows people to interact with others online by sharing opinions, insights, information, interests, and experiences.
- The number of Internet users worldwide is approaching 4 billion or roughly half the population.
- Many organizations employ social networking platforms to advertise, identify and access job candidates, improve customer service, and sell products and services.
- An increasing number of business-oriented social networking platforms are designed to encourage and support relationships with consumers, clients, potential employees, suppliers, and business partners around the world.
- Social media marketing involves the use of social networks to communicate and promote the benefits of products and services.
- Two significant advantages of social media marketing over traditional marketing are that marketers can create a conversation with viewers of their ads and that ads can be targeted to reach people with the desired demographic characteristics.
- Social media marketing involves the use of social networks to communicate and promote the benefits of products and services. The two primary objectives of social media marketers are raising brand awareness and driving traffic to a website to increase product sales.
- Organic media marketing employs tools provided by or tailored for a particular social media platform to build a social community and interact with it by sharing posts and responding to customer comments on the organization's blog and social media accounts.
- Paid media marketing involves paying a third party to broadcast an organization's display ads or sponsored messages to social network users. Two common methods of charging for paid media are cost per thousand impressions and cost per click.
- Earned media refers to media exposure an organization gets through press and social media mentions, positive online ratings and reviews, tweets and retweets, reposts (or "shares"), recommendations, and so on. Earned social media traffic enables an organization to reach more people without any additional cost.
- Viral marketing is an approach to social media marketing that encourages individuals to pass along a marketing message to others, thus creating the potential for exponential growth in the message's exposure and influence.
- Some 60 percent of employers used social media to research job candidates with half of those finding information that gave a negative impression of the candidate.
- Employers can legally reject a job applicant based on the contents of the individual's social networking profile as long as the company is not violating federal or state discrimination laws.

- Job seeking candidates should review their presence on social media and remove photos and postings that portray them in a potentially negative light. Many jobseekers delete their social media accounts altogether.
- Increasingly, consumers are using social networks to share their experiences, both good and bad, with others. Because of this, many organizations actively monitor social media networks as a means of improving customer service, retaining customers, and increasing sales.
- A social shopping platform brings shoppers and sellers together in a social networking environment in which members share information and make recommendations while shopping online.

What are some of the key ethical issues associated with the use of social networks and other social media?

- Cyberabuse is any form of mistreatment or lack of care, both physical and mental, based on the use of an electronic communications device that causes harm and distress to others.
- Nearly three-quarters of U.S. Internet users have witnessed online harassment or abuse and almost half have personally experienced it.
- Cyberharassment is a form of cyberabuse in which the abusive behavior, which involves the use of an electronic communications device, is degrading, humiliating, hurtful, insulting, intimidating, malicious, or otherwise offensive to an individual or group of individuals causing substantial emotional distress.
- Cyberstalking is also a form of cyberabuse that consists of a long-term pattern of unwanted persistent pursuit and intrusive behavior (involving the use of an electronic communications device) that is directed by one person against another that causes fear and distress in the victim.
- The National Center for Victims of Crime offers tips on how to combat cyberstalking.
- The 1994 Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act set requirements for sex offender registration and notification in the United States. It also that states create websites that provide information on sex offenders within the state.
- The Sex Offender Registration and Notification Provisions (SORNA) of the Adam Walsh Child Protection and Safety Act of 2006 set national standards that govern which sex offenders must register and what data must be captured.
- Most social networking platforms have terms of use agreements, a privacy policy, or a content code of conduct that summarizes key legal aspects regarding use of the platform. Typically, the terms state that the platform has the right to delete material and terminate user accounts that violate its policies. These policies can be difficult to enforce.
- Inappropriate material posted online includes nonconsensual posts that include intimate photos or videos of people without their permission; such posts are often referred to as “revenge porn.” This type of content is often uploaded by ex-partners with an intention to shame, embarrass, and/or harass their former partner.

- The First Amendment of the U.S. Constitution protects the right of freedom of expression from government interference, however, it does not prohibit free speech interference by private employers.
- Organizations should put in place a social media policy to avoid legal issues and set clear guidelines and expectations for employees.
- The increased risk of accidents associated with social media interaction while driving, the tendency of many social media users to become narcissist in their postings, and the ability to perform self-image manipulation are additional social media issues.

Key Terms

cost per thousand impressions (CPM)
cost per click (CPC)
cyberabuse
cyberharassment
cyberstalking
earned media
organic media marketing
paid media marketing
social media
social media marketing
social networking platform
social shopping platform
viral marketing

Self-Assessment Questions

How do individuals use social networks, and what are some practical business uses of social networking and other social media tools?

1. The number of Internet users worldwide ______________.
   a. exceeds half the population of the world
   b. is approaching 4 billion
   c. is between 2 and 3 billion
   d. is under 3 billion
2. The most popular social platform based on unique monthly visitors is ______________.
   a. YouTube
   b. Twitter
   c. Facebook
   d. Instagram
3. Millennials (born 1981 to 1997) spend the most time on social media. True or False?
4. The two primary objectives of social media marketers are ______________.
   a. developing loyal fans and increasing product sales
   b. providing market insight and generating leads
   c. generating leads and increasing product sales
   d. increasing product sales and raising brand awareness

5. _____________ employs tools provided by or tailored for a social network platform to build a social community and interact with it.

   a. Paid media marketing

   b. Organic media marketing

   c. Earned media

   d. Unearned media

6. _____________ is a measure of the number of times an ad is displayed, whether it was actually clicked on or not.

7. _____________ of employers used social media to research job candidates in 2016.

   a. Around half

   b. About one-fourth

   c. A little more than half

   d. Nearly three-quarters

8. Employers can legally reject a job applicant based on the content of the individual's social media activity only if the company is not violating federal or state discrimination laws. True or False?

What are some of the key ethical issues associated with the use of social networks and other social media?

9. Cyberharassment encompasses both cyberabuse and cyberstalking. True or False?

10. What percent of U.S. Internet users have personally experienced cyberabuse?

    a. About 25 percent

    b. Nearly one-third

    c. Just under 50 percent

    d. Over 60 percent

11. _____________ involves a long-term pattern of unwanted persistent pursuit and intrusive behavior (involving the use of an electronic communications device) that is directed by one person against another that causes fear and distress in the victim.

12. State laws that prohibit the use of social networks by registered sex offenders are effective in fighting sexual predators. True or False?

13. Which of the following measures is employed by social networking platforms to avoid the posting of objectionable material?

    a. The terms of user agreement for most social networking platforms states that the site reserves the right to delete material or terminate user accounts that violate the site's policies.

    b. Social media companies employ people to review material submitted.

    c. Other users sometimes report objectionable material.

    d. All of the above

14. The First Amendment of the U.S. Constitution protects the right to freedom of expression from private employer interference; however, it does not prohibit free speech interference by the government. True or False?

Self-Assessment Answers

1. b; 2. c; 3. False; 4. d; 5. b; 6. Impressions; 7. c; 8. True; 9. False; 10. c; 11. Cyberstalking; 12. False; 13. d; 14. False

Discussion Questions

1. Do research to identify a for-profit organization with an effective social media marketing program. What makes its program successful? Next, identify a nonprofit organization with an effective social media marketing program. What makes its program successful?
2. MIT professor Sherry Turkle has written a book, *Alone Together,* which is highly critical of social networking. She argues that the manner in which some people frenetically communicate online using Facebook, Twitter, and text messaging is a form of modern madness. Turkle thinks that under the illusion of enabling improved communications, technology is actually isolating us from true human interactions. Others disagree and argue that the use of social media has led to more communications, not less. What do you think?
3. What are the pros and cons of using paid media marketing based on cost per thousand impressions versus cost per click? Can you define any guidelines for when you might use one approach over the other?
4. Keep track of the time that you spend on social media for one week. Do you think that this is time well spent? Why or why not?
5. Develop an idea for a social media marketing campaign for one of your favorite consumer products. Brainstorm ideas for how you would turn your message viral.
6. Identify two significant advantages that social media advertising has over other forms of advertising.
7. What advice would you give a friend who is the victim of cyberstalking?
8. What measures would you use to gauge the success of a social media promotion designed to get people to try a new consumer product?
9. What type of online information about a job candidate should employment managers consider when screening candidates for an interview? Give three examples of information that might be found that should automatically disqualify a candidate from a job offer. Give three examples of online information that should increase a candidate's chances of a job offer.
10. Review your user profile on your most frequently used social media platforms. Do you think you need to make any changes to this profile? If so, what changes?
11. Check out the privacy policy of three social shopping platforms to see if they say anything about selling user data to retailers. Write a couple of sentences summarizing your findings.

What Would You Do?

Use the five-step decision-making process discussed in Chapter 1 to analyze the following situations and recommend a course of action.

1. You are a new waiter at a four-star restaurant. You and several other employees have been asked by your manager to begin posting positive messages about your dining experience at the restaurant on Facebook, Instagram, and Twitter. Truth be told, the restaurant is living on its past reputation. The menu is boring, the food is overpriced, the carpet is worn thin, and the booths need to be repaired. You would not choose to dine at the restaurant. What would you do?
2. You are 30 minutes into a job interview for your dream job—one where your college education and experience can really be applied. So far everything is going well. However, the interviewer's next question catches your breath and causes you to pause before you answer—" If I were to examine your social media postings, would I find anything that is embarrassing about you or that might indicate that you engaged in any illegal activities?" What would you say?
3. You are surprised to receive Facebook and LinkedIn friend requests from a new employee who joined your organization two weeks ago. You know nothing about the individual and are really not interested in the individual. Your first reaction is to ignore the requests but you are concerned that you will keep running into the person at work and that the situation could become awkward. What would you do?
4. You work in the human resources organization and found out through research on Facebook that a current job candidate married and divorced his high school sweetheart before graduating from college and once had his car repossessed. Is this valid grounds for dropping this candidate from further consideration? What would you do?
5. Your friend has been active on the Fancy social shopping platform. He joined with a fictitious name and personal information, and is posing as a young 20-something female. He is "following" half-a-dozen young women and commenting on the collections of items they have saved. He has shown you a number of his nasty postings and the associated—sometimes angry, sometimes hurt—responses. He invites you to join him in his charade. What would you do?

Cases

1. CDA Protects Social Media Companies

Providing material support or resources for terrorism is a crime prohibited by the USA PATRIOT Act (Title 18 of the United States Code, § 2339A and § 2339B). Victims of terrorism "may sue and shall recover threefold the damages they sustained, including attorney's fees" (18 U.S. Code § 2333). Most social media sites have explicit terms of use that prohibit content that endorses terrorism. The operators of these sites also employ workers who investigate reports of terms-of-use violations, removing material that is found to be in violation of those terms of use.

The Communications Decency Act (CDA) (47 U.S. Code § 230) states, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." This clause in the CDA provides social media companies (which host—or republish—a wide variety of speech) protection against a range of laws that might otherwise be used to hold them legally responsible for what others say and do—for instance, libel, copyright infringement, and yes, even violation of the USA PATRIOT Act. Under the CDA, lawsuits can be brought against the relevant speakers or authors, but not against the publishers.

Section 230 of the CDA has certainly stimulated the growth of social media sites; however, there have been several recent lawsuits against social media companies by the families of terrorism victims who argue that the intent of Congress when it passed the CDA was *not* to facilitate access to powerful communications tools by known terrorist organizations who use the sites to recruit, radicalize, raise funds, spread propaganda, and plan attacks.

In November 2015, a Jordanian police captain opened fire on instructors at the Jordan International Police Training Center in Amman, Jordan, killing five people, including two Americans. The terrorist group ISIS claimed credit for the carnage and promoted it on social media. The families of the two Americans killed in the incident filed a lawsuit against Twitter in January 2016. The families alleged that Twitter's failure to halt ISIS propaganda was a violation of U.S. anti-terrorism laws and that Twitter was instrumental in the fundraising and recruitment efforts of ISIS. The plaintiffs, however, did not specifically charge that ISIS used Twitter to recruit the person who committed the terrorist attack that injured the plaintiffs or that Twitter was used to plan the attack. The U.S. district judge overseeing the case ruled that "As horrific as these deaths were, under the CDA, Twitter cannot be treated as a publisher or speaker of ISIS's hateful rhetoric and is not liable under the facts alleged."

A similar lawsuit was filed in June 2016 against Facebook, Google, and Twitter by the family of Nohemi Gonzalez, the only American among 130 killed in coordinated attacks by ISIS at a Paris soccer stadium and concert venue in November 2015. Gonzalez's family blamed the social media companies for providing "material support" to the terrorists, claiming that the terrorists use the social networks "as a tool for spreading extremist propaganda, raising funds, and attracting new recruits." The attorney for the family protested, "These companies are not doing a good enough job from keeping the terrorists from using their network." Furthermore, the family argued, in some cases, the social media sites place ads next to ISIS content and share with the terrorist group the revenue generated from those ads. Regardless of the outcome of the court case, the family's arguments might be successful in the court of public opinion. If so, social media companies might choose to increase their efforts to restrict use of their networks by terrorists even if they are not required by law to do so.

A June 2016 mass shooting killed 49 people and injured 68 others at the Pulse nightclub in Orlando, Florida. Lawyers representing the families of the victims filed suit in December 2016 against Facebook, Twitter, and Google. They alleged that the three companies "purposefully, knowingly, or with willful blindness" provided "material support" to a foreign terrorist organization whose social media inspired a terrorist to target the LGBT club. The lawyers filing the lawsuit intend to follow a different strategy and show that by matching users' content with targeted advertising, the social media sites are, in effect, producing their own, novel content, and profiting from terrorist users' content.

Critical Thinking Questions

1. Do you believe that social media companies are doing enough to shut off the communications of terrorist groups? Do you have any ideas for actions they could take that would help solve the problem?
2. Should U.S. anti-terrorism laws take precedence over the "safe harbor" provisions of the Communications Decency Act? Why or why not?
3. Do research to learn the current status of the Gonzalez and Pulse lawsuits were settled. Write a brief summary of your findings, and discuss if you are satisfied with the results.

Sources: "2 Americans Among 5 Killed In Rare Jordan Police Shooting," *Chicago Tribune*, November 9, 2015, www.chicagotribune.com/news/nationworld/ct-americans-killed-jordan-officer-shooting-20151109-story.html; Jeff John Roberts, "Twitter Sued by Widow of ISIS Victim," *Fortune*, January 14, 2016, http://fortune.com/2016/01/14/twitter-isis-lawsuit/; Jeff John Roberts, "These Popular Social Media Sites Are Getting Sued Over Alleged Support for ISIS," *Fortune*, June 16, 2016, http://fortune.com/2016/06/16/social-media-isis-lawsuit/; Steven Porter, "Pulse Victims Lawsuit: Did Social Media Provide 'Material Support' for Terrorism," *Christian Science Monitor*, December 20, 2016, www.csmonitor.com/USA/2016/1220/Pulse-victims-lawsuit-Did-social-media-provide-material-support-for-terrorism; Saqib Shah, "Twitter Not Liable For The Rise of Isis, Rules Federal Court," *Digital Trends*, August 11, 2016, www.digitaltrends.com/social-media/twitter-isis-lawsuit-dismissed/; Cyrus Farivar, "It'll Be Very Hard for Terrorism Victim's Family to Win Lawsuit Against Twitter," *Ars Technica*, June 17, 2016, https://arstechnica.com/tech-policy/2016/06/itll-be-very-hard-for-terrorism-victims-family-to-win-lawsuit-against-twitter/.

2. Google Losing Revenue in Dispute over Placement of Ads

Google AdWords is an advertising service for companies who want their ads presented on the pool of over 2 million websites that constitute the Google Display Network. Google ads are bought and placed online using an automated system called programmatic advertising that finds appropriate websites on which to place each ad. Placement depends on such factors as keywords used in the ads and the interests and demographics of the target audience.

YouTube was bought by Google for $1.7 billion in November 2006. Today, YouTube has over a billion active users and everyday people spend hundreds of millions of hours watching video on YouTube. Such massive viewership has made it a key member of the Google Display Network.

YouTube's popularity stems from its massive and diverse library of video spanning everything from amateur video clips of kittens to professionally produced TV clips. While this diversity is a huge asset for Google, it has also forced the company to defend the placement of ads alongside objectionable content, including videos promoting anti-Semitism, heterosexism, misogynism, racism, and terrorism. Companies advertising on YouTube are concerned that such placement creates the impression that they support pornography or hate speech. And because YouTube splits advertising revenue with its users, advertisers risk directly funding creators of this objectionable material. Those who post videos can earn up to $7.60 for each 1,000 views that an advertisement attracts. Some of the most viewed extremist clips on YouTube receive nearly one million hits. Major brands such as AT&T, Coca-Cola, Johnson & Johnson, L'Oreal, McDonald's, and Verizon have begun withholding ad dollars saying that they can no longer advertise on YouTube until Google can ensure that this won't happen again. The financial hit to Google from the boycott is significant—estimated at as high as $750 million.

With some 400 hours of user-generated content uploaded to YouTube every minute, Google has asserted that it simply does not have the resources to police that flood of content in real time. As a result, inappropriate and offensive content continues to be posted. This has advertisers, who place a high priority on protecting their brands, increasingly concerned. Google's efforts to solve the problem include the hiring of "significant numbers" of new workers to review YouTube content and flag inappropriate content as well as making an ongoing investment in artificial intelligence that the company hopes will help it fine-tune its ad placement service. Google has considerable incentive to resolve the concerns of advertisers as ad system sales brought in more than $79 billion in revenue to the company in 2016.

Critical Thinking Questions

1. Should Google take a more active approach in censoring its content providers? If it does, is it possible that Google could run afoul of Title II of the Digital Millennium Copyright Act and lose its legal immunity for the actions of its users?
2. How might Google deploy advanced technologies to identify content that is objectionable?
3. Can/should Google provide advertisers with guarantees about what type of content their ads will appear next to? How could such guarantees be written so that they are enforceable?

Sources: Media Matters Staff, "Advertisers Are Fleeing YouTube to Avoid 'Directly Funding Creators of Hateful' Content," *Media Matters*, March 24, 2017, https://mediamatters.org/blog/2017/03/24/advertisers-are-fleeing-google-avoid-directly-funding-creators-hateful-content/215801; Michael Liedtke, "Google's YouTube Losing Major Advertisers Upset with Videos," *AP News*, March 22, 2017, http://bigstory.ap.org/article/9c38f2c988f546a78e84511207ff8cea/googles-youtube-losing-major-advertisers-upset-videos; Holman W. Jenkins, Jr., "Google's Too-Darn-Bad Scandal," *Wall Street Journal*, March 28, 2017, https://www.wsj.com/articles/googles-too-darn-bad-scandal-1490740494; Suzanne Vranica, "TV Networks See an Opportunity in Google Ad Backlash," *Wall Street Journal*, March 28, 2017, https://www.wsj.com/articles/tv-networks-spy-opportunity-in-google-ad-backlash-1490697000; and Mark Bridge, "Google Lets Anti-Semitic Videos Stay on YouTube," *The Times*, March 18, 2017, http://www.thetimes.co.uk/article/google-lets-antisemitic-videos-stay-on-youtube-t83x06d2v.

End Notes

[1] Daniel Nations, "What Is Social Media? Explaining the Big Trend," *Lifewire*, March 9, 2017, https://www.lifewire.com/what-is-social-media-explaining-the-big-trend-3486616.

[2] "Internet Usage Stats," *Internet World Statistics*, March 25, 2017, www.internetworldstats.com/stats.htm.

[3] "2016 Nielsen Social Media Report," The Nielsen Company, www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2017-reports/2016-nielsen-social-media-report.pdf (accessed March 28, 2017).

[4] Ibid.

[5] "Social Media Ads to Reach $50 Billion By 2019," *Reuters*, December 4, 2016, www.reuters.com/article/us-advertising-forecast-idUSKBN13U001.

[6] "Global Advertising Revenue Forecasts Spring Update," Magna, November 28, 2016, http://magnaglobal.com/global-advertising-revenue-forecasts-spring-update/.

[7] "Social Media Principles," www.coca-colacompany.com/stories/online-social-media-principles, The Coca-Cola Company (accessed April 5, 2017).

[8] "Coca-Cola Reaffirms Social Media Marketing 'Crucial' to Sales," Brafton, March 21, 2013, www.brafton.com/news/coca-cola-reaffirms-social-media-marketing-crucial-to-sales.

[9] Ramona Sukhraj, “The Advantages of Viral Marketing,” *Impact*, September 14, 2016, https://www.impactbnd.com/blog/the-advantages-of-viral-marketing.

[10] Roy Mauer, “Know Before You Hire: 2017 Employment Screening Trends,” Society for Human Resource Management, January 25, 2017, https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/2017-employment-screening-trends.aspx.

[11] Bryan Haines, “14 Amazing Social Media Service Examples (And What You Can Learn from Them),” Buffer Social, December 29, 2015, https://blog.bufferapp.com/social-media-customer-service.

[12] Alicia Boler-Davis, “How GM Uses Social Media to Improve Cars and Customer Service,” *Harvard Business Review*, February 12, 2016, https://hbr.org/2016/02/how-gm-uses-social-media-to-improve-cars-and-customer-service.

[13] Stuffpit, “Earn Money Recommending Products,” www.stuffpit.com/stuff/earn (accessed July 2, 2011).

[14] Amanda Lenhart, Michele Ybarra, Kathryn Zickuhr, and Myeshia Price-Feeney, “Online Harassment, Digital Abuse, and Cyberstalking in America,” Data & Society Research Institute, November 21, 2016, https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf.

[15] Amanda Lenhart, Michele Ybarra, Kathryn Zickuhr, and Myeshia Price-Feeney, “Online Harassment, Digital Abuse, and Cyberstalking in America,” Data and Society Research Institute, November 21, 2016, https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf.

[16] Joey L. Blanch and Wesley L. Hsu, “An Introduction to Violent Crime on the Internet,” *Cyber Misbehavior*, May 2016, Vol 64 No 3, https://www.justice.gov/usao/file/851856/download.

[17] “Online Harassment and Cyberstalking,” Online Rights Privacy Clearing House, December 14, 2016, https://www.privacyrights.org/consumer-guides/online-harassment-cyberstalking.

[18] “Federal Stalking Laws,” Stalking Resource Center, https://victimsofcrime.org/our-programs/stalking-resource-center/stalking-laws/federal-stalking-laws (accessed April 9, 2017).

[19] Matt Smith, “Indiana Can’t Kick Sex Offenders Off Social Media, Court Says,” CNN, January 23, 2013, www.cnn.com/2013/01/23/tech/sex-offenders-social-media.

[20] Christina Horst, “The 2006 Sex Offender Registration and Notification Act: What Does It Mean for Your Law Enforcement Agency?” *Police Chief*, November 2007, www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1317&issue_id=112007.

[21] GovTrack.us, “H.R. 4472 (109th): Adam Walsh Child Protection and Safety Act of 2006,” www.govtrack.us/congress/bills/109/hr4472/text.

[22] Ibid.

[23] “Background Summary of SORNA,” National Conference of State Legislatures, March 21, 2017, http://www.ncsl.org/documents/statefed/Background_on_SORNA_March2017.pdf.

[24] U.S. Government Accountability Office, “Sex Offender Registration and Notification Act: Jurisdictions Face Challenges to Implementing the Act, and Stakeholders Report Positive

and Negative Effects," GAO Highlights, February 2013, http://www.gao.gov/products/GAO-13-211.

[25] Thomas Nibbens-Giff, "Investigation Has Identified 1,200 Members of Marine Group Involved in Nude Photo Sharing," *The Washington Post*, March 17, 2017, https://www.washingtonpost.com/news/checkpoint/wp/2017/03/17/investigation-has-identified-1200-members-of-marine-group-involved-in-nude-photo-sharing/.

[26] Niraj Chokshi, "Facebook Announces New Ways to Prevent 'Revenge Porn'", *New York Times*, April 5, 2017, https://www.nytimes.com/2017/04/05/us/facebook-revenge-porn.html.

[27] Jon Hyman, "What the First Amendment Really Says," *Workforce*, September 8, 2016, www.workforce.com/2016/09/08/free-speech-social-media-job/.

[28] Alfred Ng, "Bank of America Employee Fired after Racist Facebook Rant, Thousands of Social Media Complaints Sent to Her Bosses," *New York Daily News*, June 3, 2016, www.nydailynews.com/news/national/bank-america-employee-fired-racist-facebook-rant-article-1.2658891.

[29] Dara Fontein, "How to Write a Social Media Policy for Your Company," *Hootsuite*, February 23, 2017, https://blog.hootsuite.com/social-media-policy-for-employees/.

[30] "Employee Social Media Policy Sample," *Workable*, https://resources.workable.com/social-media-company-policy (accessed April 1, 2017).

[31] "Distracted Driving Facts Learn the Facts about Distracted Driving," End Distracted Driving, http://www.enddd.org/the-facts-about-distracted-driving/ (accessed May 9, 2017).

[32] "Fight the Filter: Snapchat Selfies Distort User's Self-Image," *USA Today*, August 18, 2016, http://college.usatoday.com/2016/08/18/fight-the-filter-snapchat-selfies-distort-users-self-image/.

CHAPTER 10

ETHICS OF IT ORGANIZATIONS

QUOTE

> *Corporate executives and business owners need to realize that there can be no compromise when it comes to ethics, and there are no easy shortcuts to success. Ethics need to be carefully sown into the fabric of their companies.*
>
> —Vivek Wadhwa, academic, entrepreneur, and syndicated columnist for *The Washington Post*

Rafal Olechowski/Shutterstock.com

ORGANIZATIONS BEHAVING BADLY

Executive Order 11246, which was signed by President Lyndon B. Johnson in 1965, states that “It is the policy of the Government of the United States to provide equal opportunity in Federal employment for all qualified persons, to prohibit discrimination in employment because of race, creed, color, or national origin, and to promote the full realization of equal employment opportunity through a positive, continuing program in each executive department and agency. The policy of equal opportunity applies to every aspect of Federal employment policy and practice."[1] Violations of the order may result in cancellation, suspension, or termination of contracts, withholding of progress payments, debarment, and other sanctions. The Age Discrimination in Employment Act of 1967 protects job applicants and employees of age 40 years and older from discrimination on the basis of age in hiring, promotion, discharge, compensation, or terms, conditions or privileges of employment.

In spite of these regulations, the tech industry in the United States has a high percentage of white and Asian male employees and executives, as well as a documented tendency toward hiring younger job applicants and letting go of older workers. In addition, in many tech organizations, large salary gaps exist between male and female workers in the same jobs. For example, female software developers make about 83 percent of what male ones earn. There are similar wage gaps in other jobs, such as programmers and front-end engineers.[2] The following are just a few examples of discrimination-related investigations and lawsuits that have hit the tech industry in recent years:

- Google, Oracle, and Qualcomm have all been the subject of U.S. Department of Labor investigations for paying white men more than women and minorities. Qualcomm has already agreed to a $19.5 billion class-action settlement in connection with the investigation into its employment practices; the Google and Oracle investigations are ongoing.[3,4]
- Palantir, a data analytics company, was sued by the Department of Labor for alleged discrimination against Asian job applicants in its hiring processes. In April 2017, the Department of Labor and Palantir entered into a consent decree to settle the allegations. As part of the agreement, Palantir must pay almost $1.7 million in back wages and other monetary relief to affected applicants. The company is also required to extend job offers to eight of those applicants.[5,6]

- Since 2012, almost 90 age-related complaints have been filed against several IT firms, including Apple, Cisco Systems, Facebook, Google, Hewlett-Packard, Intel, LinkedIn, Oracle, Yahoo, and Twitter. Most of the claims cite wrongful termination, while others cite hiring or promotion practices.[7]

Tech firms typically make great efforts to ensure their written policies comply with antidiscrimination laws; however, that does mean that the policies are being implemented effectively at all companies. Thus, having such policies does not necessarily shield a company from a discrimination suit. Many tech firms have begun publishing diversity figures and have launched initiatives to address these issues, but, unfortunately, few have shown much progress. Visit the website of three large tech companies and search for a statement of their equal employment policy and practices. Look for any documentation on the number of women and minorities employed. What are your findings?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What key legal and ethical issues are associated with the use of contingent workers, H-1B visa holders, and offshore outsourcing companies?
2. What is whistle-blowing, and what ethical issues are associated with it?
3. What is green computing, and what are organizations doing to support this initiative?

USE OF CONTINGENT WORKERS

The Bureau of Labor Statistics defines **contingent work** as a job situation in which an individual does not have an explicit or implicit contract for long-term employment.[8] A firm is likely to use contingent IT workers if it experiences pronounced fluctuations in its technical staffing needs. For example, contingent workers may be hired as consultants on an organizational restructuring project, as technical experts on a product development team, and as supplemental staff for many other short-term projects, such as the design and installation of a new information system. Typically, these workers join a blended team of full-time employees and other contingent workers for the life of the project and then move on to their next assignment. Whether they work, when they work, and how much they work depends on the company's need for them. They have neither an explicit nor an implicit contract for continuing employment. Organizations can obtain contingent workers through temporary staffing firms, employee leasing organizations, and professional employer organizations (PEOs).

Temporary staffing firms recruit, train, and test job seekers in a wide range of job categories and skill levels, and then assign them to clients as needed. Temporary employees are often used to fill in during staff vacations and illnesses, handle seasonal workloads, and help staff special projects. However, they are not employees of the client company, so they are not eligible for company benefits such as vacation, sick pay, and medical insurance. Temporary working arrangements may appeal to people who want maximum flexibility in their work schedules, as well as a variety of work experiences. Other workers take temporary work assignments because they are unable to find more permanent work.

In **employee leasing**, a business (called the subscribing firm) transfers all or part of its workforce to another firm (called the leasing firm), which handles all human-resource-related activities and costs, such as payroll, training, and the administration of employee benefits. The subscribing firm leases these workers, but they remain employees of the leasing firm. Employee leasing creates a **coemployment relationship**, in which two employers have actual or potential legal rights and duties with respect to the same employee or group of employees. Employee leasing firms are subject to special regulations regarding workers' compensation and unemployment insurance. Because the workers are technically employees of the leasing firm, they may be eligible for some company benefits through the leasing firm. Once the relationship between the employee leasing firm and its client ends, the leased employees remain with the leasing firm and move on to other projects with new clients.

A **professional employer organization (PEO)** is a business entity that coemploys the employees of its clients and typically assumes responsibility for all human resource management functions. The PEO typically remits wages and withholdings of the worksite employees and reports, collects, and deposits employment taxes with local, state, and federal authorities. The PEO also issues the Form W-2 for the compensation paid by it under its EIN (Employer Identification Number). The client company remains responsible for directing and controlling the daily activities of the employees, tracking actual hours worked and reporting them to the PEO for payment processing, and ensuring that payroll funds are paid to the PEO. The exact terms of the arrangement are specified in a client service agreement.

The client maintains a long-term investment and commitment to the employees, but uses the PEO as a means to outsource the human resource activities. If the agreement between the client company and the PEO is terminated, the workers continue to be employed by the client. By assigning the nonrevenue-producing administrative tasks to the PEO, the client company can focus on managing and growing its business while letting administrative tasks be handled by human resource experts, ideally at a lower total cost.

The Gig Economy

The term *gig*, which originated in the entertainment business, refers to a short-term job. The Bureau of Labor Statistics refers to a gig as a "a single project or task for which a worker is hired—often through a digital marketplace—to work on demand."[9] The **gig economy** refers to a work environment in which temporary positions are common and organizations contract with independent workers for short-term engagements. In the gig economy, instead of earning a regular hourly wage, workers get paid for specific gigs, such as complete testing of a unit of software code, writing end user documentation, or delivering a training class via webinar.

Employers are desperate for highly qualified workers with specialized skills. And thanks to the power of the Internet and the nature of much IT work, those individuals may be located anywhere in the world. Many of those workers are willing to work a gig for highly competitive rates. Online staffing websites such as 99 Designs, Freelancer, Guru, Toptal, Witmart, and over a dozen others can help organizations find these workers. Some of these websites draw from a database of over one million professionals, enabling organizations to find the talent they need with just a few clicks. Organizations can post their project and have contractors bid on it, or they can search for workers and contact those they are interested in directly. Some sites vet the workers to some degree, or at least let potential employers view feedback and ratings of prior clients. The sites typically handle all payment services.

Independent Contractors

An **independent contractor** is an individual who provides services to another individual or organization according to terms defined in a written contract or within a verbal agreement. A study by Intuit predicted that by 2020, more than 40 percent of American workers would be independent contractors.[10] There are many factors driving this trend toward the use of independent contractors, as shown in Table 10-1.

TABLE 10-1 Factors behind the trend toward independent contractors

From the employee's perspective	From the employer's perspective
Freedom to select from among temporary jobs and projects around the world	Ability to choose the best individuals for a specific project from a larger pool of candidates than that available in a given geographic area
Opportunity to change "jobs" frequently	Financial pressure to reduce staff and associated costs, such as payroll and benefits as well as costs associated with office space and training
Greater flexibility in terms of work hours and location where work is performed	Enables organization to focus on its core functions and on building its business

Organizations that use contingent workers must be extremely careful how they pay and treat those workers, or they run the risk of getting dragged into a class action lawsuit over misclassification of workers. Table 10-2 details some of the factors that come into play in classifying a worker as either an employee or an independent contractor.

TABLE 10-2 Factors that are considered in classifying a worker as either an employee or an independent contractor

Employee	Independent contractor
Receives net salary after employer has withheld income, Social Security, and Medicare taxes	No income, Social Security, or Medicare taxes are withheld from paycheck; worker must make arrangements to pay his or her own taxes
Receives a W-2 form from the employer for the purposes of filing federal, state, and local taxes	Receives a form 1099-MISC for amounts exceeding $599 of nonemployee income for the purposes of filing federal, state, and local income taxes
Eligible for employment benefits, such as health and disability insurance, vacation and holiday pay, and contributions to an employee-sponsored retirement account	Receives no employment benefits from the employer
Eligible to receive unemployment compensation after layoff or termination	Not eligible for unemployment compensation benefits
Covered by federal and state wage and hour laws, such as those related to minimum wage and overtime	Paid according to the terms of the contract, typically does not receive overtime pay
Can receive worker's compensation benefits for any workplace injury	Not eligible for worker's compensation benefits
Protected by workplace safety and employment antidiscrimination laws	Not protected by employment antidiscrimination and workplace safety laws
Unless employment is "at will," can be terminated by the employer only for just cause and with prior notice	Unless the consulting contract is for a specified term, can be let go by the employer for any reason, at any time
Employer has right to control or direct not only the result of the work but also how it will be done and when	Client has the right to control or direct only the result of the work; other than that, worker operates independently and decides what will be done and how the work will be accomplished
Works hours set by the employer	Sets own work hours
All equipment, materials, and tools are provided to perform the work	Provides his or her own equipment, materials, and tools

Advantages of Using Contingent Workers

When a firm employs a contingent worker, it does not usually have to provide benefits such as insurance, paid time off, and contributions to a retirement plan. A company can easily adjust the number of contingent workers it uses to meet its business needs and can release contingent workers when they are no longer needed. An organization cannot usually do the same with full-time employees without creating a great deal of ill will and negatively impacting employee morale. Moreover, because many contingent workers are already specialists in a particular task, a firm does not customarily incur training costs for contingent workers. Therefore, the use of contingent workers can enable a firm to meet its staffing needs more efficiently, lower its labor costs, and respond more quickly to changing market conditions.

Disadvantages of Using Contingent Workers

One downside to using contingent workers is that those workers may not feel a strong connection to the company for which they are working. This can result in a low commitment to the company and its projects, along with a high turnover rate. Although contingent workers may already have the necessary technical training for a temporary job, many contingent workers gain additional skills and knowledge while working for a particular company; those assets are lost to the company when a contingent worker departs at a project's completion.

Deciding When to Use Contingent Workers

When an organization decides to use contingent workers for a project, it should recognize the trade-off it is making between completing a single project quickly and cheaply versus developing people within its own organization. If the project requires unique skills that are probably not necessary for future projects, there may be little reason to invest the additional time and costs required to develop those skills in full-time employees. Or, if a particular project requires only temporary help that will not be needed for future projects, the use of contingent workers is a good approach. In such a situation, using contingent workers avoids the need to hire new employees and then fire them when staffing needs decrease.

However, organizations should carefully consider whether or not to use contingent workers when those workers are likely to learn corporate processes and strategies that are key to the company's success. It is next to impossible to prevent contingent workers from passing on such information to subsequent employers. This can be damaging if the worker's next employer is a major competitor.

Although using contingent workers is often the most flexible and cost-effective way to get a job done, their use can raise ethical and legal issues about the relationships among the staffing firm, its employees, and its customers—including the potential liability of a staffing firm's clients for withholding payroll taxes, payment of employee retirement benefits and health insurance premiums, and administration of workers' compensation to the staffing firm's employees. Depending on how closely workers are supervised and how the job is structured, contingent workers may be viewed as permanent employees by the Internal Revenue Service, the Department of Labor, or a state's workers' compensation and unemployment agencies.

Review the manager's checklist in Table 10-3 for questions that pertain to the use of contingent workers. The preferred answer to each question is *yes*. Recognize, however, that worker classification rules are extremely difficult to apply. Each major labor and employment statue—the National Labor Relations Act, the Civil Rights Act, the Fair Labor Standards Act, and the Employee Retirement Income Security Act has its own definition of "employee" and its own way of distinguishing between employees and independent contractors. Adding to the complication is the fact that there are different rules promulgated by the Department of Labor, the Internal Revenue Service, and the Office of Workers' Compensation Programs.

TABLE 10-3 Manager's checklist for the use of contingent employees

Question	Yes	No
Have you reviewed the definition of an employee in your company's policies and pension plan documents to ensure it is not so broad that it encompasses contingent workers, thus entitling them to benefits?		
Are you careful not to use the same contingent workers on an extended basis? Do you make sure the assignments are finite, with break periods in between?		
Do you use contracts that specifically designate workers as contingent workers?		
Are you aware that the actual circumstances of the working relationship determine whether a worker is considered an employee in various contexts, and that a company's definition of a contingent worker may not be accepted as accurate by a government agency or court?		
Are you and other managers and workers aware that staffing firm employees are covered by antidiscrimination laws and therefore you cannot discriminate against them on the basis of race, color, religion, sex, national origin, or disability?		
Do you avoid telling contingent workers where, when, and how to do their jobs and instead work through the contingent worker's manager to communicate job requirements?		
Do you request that contingent workers use their own equipment and resources, such as computers and email accounts?		
Do you avoid training your contingent workers?		
When leasing employees from an agency, do you let the agency do its job? Do you avoid asking to see résumés and getting involved with compensation, performance feedback, counseling, or day-to-day supervision?		
If you lease employees, do you use a leasing firm that offers its own benefits plan, deducts payroll taxes, and provides required insurance?		

The cost of misclassifying workers can run into the millions. For example, a worker that was classified as an independent contractor may sue a company claiming that he or she is actually a legal employee and, as such, is entitled to various additional compensation and benefits, such as overtime or profit sharing. For large organizations, an individual worker's lawsuit can easily turn into a class action lawsuit involving dozens or even hundreds of workers.

CRITICAL THINKING EXERCISE: GOOGLE MISMANAGES INDEPENDENT CONTRACTORS

A former Google worker sued the tech giant and the online staffing firm oDesk (now part of Upwork, a global freelancing platform) alleging that he and others were misclassified as independent contractors rather than Google employees. According to the suit, the employee was paid as an independent contractor through oDesk and assigned projects that were impossible for him to complete in the maximum 30 hours per week that he was authorized to bill. This forced him to work additional hours on his own time, without the benefit of overtime pay to which he was legally entitled to under the Fair Labor Standards Act. Google also provided the worker with a mobile phone, tablet, and laptop computer while he worked at Google offices in New York. Google further required that the worker use Google proprietary software and conform to the employee code of conduct in regards to absenteeism, blogging, and dress code. The worker complained about nonpayment of the additional work hours and attempted to renegotiate his contract. Google ended his contract and hired another independent contractor. The worker filed a class action lawsuit against Google and oDesk on behalf of himself and other workers Google treated in the same manner.[11] A private settlement with undisclosed terms was reached in 2015. How should Google have managed this worker differently and avoided a (likely) expensive class action lawsuit? Would it be unethical for other firms to avoid hiring this worker based on his action of filing a class action lawsuit?

H-1B WORKERS

An **H-1B visa** is a temporary work visa granted by the U.S. Citizenship and Immigration Services (USCIS) for people who work in specialty occupations—jobs that require at least a four-year bachelor's degree in a specific field, or equivalent experience. People working in the United States on H-1B visa are referred to as "nonimmigrant workers" because they are in the country on a temporary work visa; they are not being granted a visa to immigrate to the United States. Many companies turn to H-1B workers to meet critical business needs or to obtain essential technical skills and knowledge that they claim cannot be readily found in the United States. An individual can work for a U.S. employer as an H-1B employee for a maximum continuous period of six years.[12] The top countries of birth for H-1B workers in 2015 were India with 70.9 percent of all approved H-1B petitions and China with 9.7 percent.[13] Table 10-4 shows the cities with the most H-1B workers in 2016.

TABLE 10-4 Cities with the most H-1B workers

City	H-1B visas certified 2016
New York City, NY	36,122
Houston, TX	17,432
San Francisco, CA	14,355
Atlanta, GA	11,507
San Jose, CA	10,955
Chicago, IL	10,278
Sunnyvale, CA	8,344
Charlotte, SC	6,942
Irving, TX	6,695
Dallas, TX	6,591

Source: "2016 H-1B Visa Report: Top H-1b Visa Work City," myvisajobs.com, http://www.myvisajobs.com/Reports/2016-H1B-Visa-Category.aspx?T=WC.

Each year the U.S. Congress sets an annual cap on the number of H-1B visas to be granted—although the number of visas actually issued often varies greatly from this cap. Since 2004, the cap has been set at 65,000, with an additional 20,000 visas available for foreign graduates of U.S. universities with advanced degrees. The cap only applies to certain IT professionals, such as programmers and engineers at private technology companies. A petition to extend an H-1B nonimmigrant's period of stay, change the conditions of the H-1B nonimmigrant's current employment, or request new H-1B employment for an H-1B worker already in the United States does not count against the H-1B fiscal year cap. In addition, a large number of foreign workers are exempt from the cap, including scientists hired to teach at American universities, work in government research labs, or work for nonprofit organizations.

Foreign professionals can convert their H-1B visas into permanent green cards, which grants them authorization to live and work in the United States on a permanent basis, provided their employers file the necessary paperwork. This process can take a few years to complete, but the federal government allows H-1B professionals to obtain additional one-year H-1B visas to remain in their jobs until they get approval for their green card. This process also results in an increase of the total number of H-1B visas above the 85,000 cap.

In 2015, USCIS approved a total of 275,317 H-1B petitions submitted on behalf of alien workers. Of these, 70,902 initial employment H-1B petitions plus an additional 112,174 petitions for continuing employment were approved for workers in computer-related occupations.[14]

Using H-1B Workers Instead of U.S. Workers

In order to compete in the global economy, U.S. firms must be able to attract the best and brightest workers from all over the world. Most H-1B workers are brought to the United States to fill a legitimate gap that cannot be filled from the existing pool of workers. However, there are some managers who reason that as long as skilled foreign workers can be found to fill critical positions, why invest thousands of dollars and months of training to develop the available pool of U.S. workers? Although such logic may appear sound for short-term hiring decisions, it does nothing to develop the strong core of permanent IT workers that the United States will need in the future. Heavy reliance on the use of H-1B workers can lessen the incentive for U.S. companies to educate and develop their own workforces.

Companies using H-1B workers, as well as the workers themselves, must also consider what will happen at the end of the six-year H-1B visa term. The stopgap nature of the visa program can be challenging for both sponsoring companies and applicants. If a worker is not granted a green card, the firm can lose a worker without having developed a permanent employee. Many of these foreign workers, finding that they are suddenly unemployed, are forced to uproot their families and return home.

Gaming the H-1B Visa Program

Even though companies applying for H-1B visas must offer a wage that is at least 95 percent of the average salary for the occupation, some companies use H-1B visas as a way to lower salaries. Because wages in the IT field vary substantially, unethical companies can get around the average salary requirement. Determining an appropriate wage is an imprecise science at best. For example, an H-1B worker may be classified as an entry-level IT employee and yet fill a position of an experienced worker who would make $10,000 to $30,000 more per year.

Companies that employ H-1B workers are required to declare that they will not displace American workers. But companies are exempt from that requirement if 15 percent or more of their workers are on H-1B visas and the H-1B workers are paid at least $60,000 a year. Thus, H-1B workers at outsourcing firms often receive wages slightly above $60,000—below what similarly skilled American technology professionals earn, allowing those firms to offer services to U.S. companies at a lower cost, undercutting U.S. workers.[15] The majority of people hired with H-1B visas in 2015 were hired primarily as computer programmers and systems analysts, and were paid a median salary of between $61,131 and $71,150.[16] However, the median salary for all U.S. computer programmers was $79,840, and for systems analysts, the median salary was $87,220. Table 10-5 shows the employers who received approval for the most H-1B visas in 2015.

TABLE 10-5 Top H-1B visa employers in 2015

Company	Approved H-1B petitions	Median salary paid H-1B workers
Cognizant Technical Solutions	15,680	$61,131
Infosys	8,991	$65,631
Tata Consultancy Services	6,339	$65,600
Accenture	5,793	$67,100
Wipro Ltd.	4,803	$64,522
HCL America	2,776	$67,350
Tech Mahindra	2,657	$65,437
IBM India	2,500	$71,150

Source: Dawn Kawamoto, "8 Biggest H-1B Employers in 2015," InformationWeek, March 24, 2016, www.informationweek.com/government/8-biggest-h-1b-employers-in-2015/d/d-id/1324807?image_number=9.

The Need for H-1B Workers

The heads of many U.S. companies complain that they have trouble finding enough qualified IT employees and have urged the USGIS to loosen restrictions on visas for qualified workers. Meanwhile, unemployed and displaced IT workers in the United States, as well as other critics, challenge whether the United States needs to continue importing tens of thousands of H-1B workers every year.

The Bureau of Labor Statistics (BLS) estimates that as of 2014, there were 4.3 million people employed in the United States in the IT-related positions shown in Table 10-6. The BLS expects this sector to add close to 532,000 new jobs between 2014 and 2024—or an average of about 53,000 new jobs per year over the decade.

TABLE 10-6 IT jobs: 10-year forecast

Position	Employment 2014 (000)	Employment 2024 (000)	Employment change (000)	2016 Median wage ($)
Computer & information system managers	348.5	402.2	53.7	$135,800
Computer & information research scientist	25.6	28.3	+2.7	$111,840
Computer hardware engineer	77.7	80.1	2.4	$115,080
Computer network architect	146.2	158.9	+12.7	$101,210
Computer programmer	328.6	302.1	–26.5	$79,840
Computer user support specialist	585.9	661.0	75.1	$49,390
Computer network support specialist	181.0	194.6	13.6	$62,670
Computer operator	61.1	49.5	–11.6	$42,270
Computer, automated teller, and office machine repairers	131.6	134.8	3.2	$37,100
Computer systems analyst	567.8	686.4	+118.6	$87,220
Computer science teachers, postsecondary	43.4	47.2	3.8	$77,570
Database administrator	120.0	133.4	+13.4	$84,950
Information security analyst	82.9	97.7	+14.8	$92,600
Network and computer systems administrator	382.6	412.8	+30.2	$79,700
Software developer, applications	718.4	853.7	135.3	$100,080
Software developer, systems software	395.6	447.0	51.3	$106,860
Web developer	148.5	188.0	+39.5	$66,130
Total	**4,345.4**	**4,877.7**	**+532.3**	

Source: "Computer and Information Technology Occupations," Bureau of Labor Statistics, https://www.bls.gov/ooh/computer-and-information-technology/mobile/home.htm, accessed April 20, 2017.

Figure 10-1 shows the forecasted number of new job openings by 2024 for selected IT positions, as well as the median 2016 salaries associated with these positions.[17] (Of course, it must be recognized that any 10-year forecast is subject to a wide range of uncertainty). Not shown in BLS labor forecasts are the number of workers to fill new positions such as artificial intelligence/machine learning architect, big data scientist, and cloud services engineer. The demand for workers to fill these positions is expected to be high.

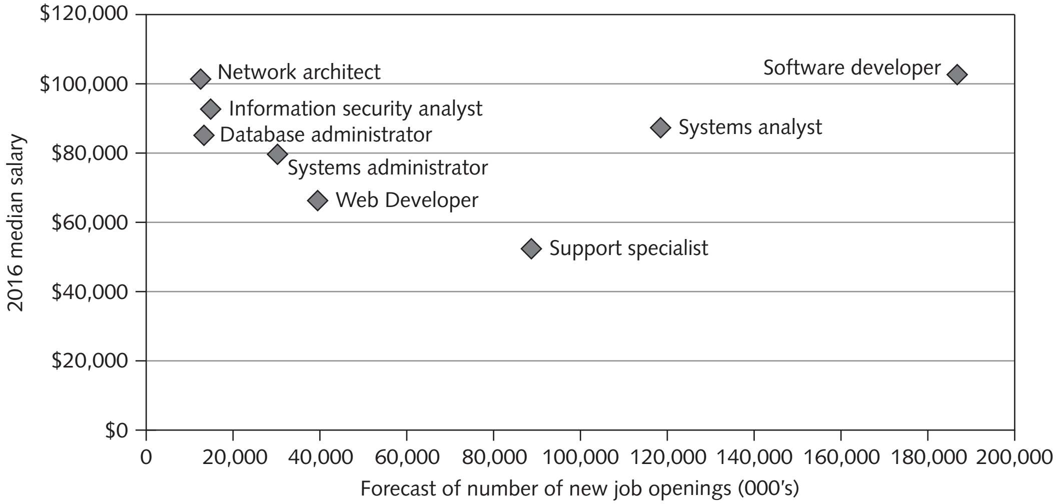


FIGURE 10-1 Occupational outlook for selected IT positions

Source: "Computer and Information Technology Occupations," Bureau of Labor Statistics

IT firms and many other organizations cite concerns about a shortfall in the number of skilled U.S. workers as justification for hiring H-1B workers, and many tech companies have advocated for an increase in the H-1B hiring cap. However, based on the data from the National Center for Education Statistics (shown in Figure 10-2), there are some 130,000 new computer and information science graduates each year[18] to fill what the BLS projects as a need of roughly 53,000 new U.S. tech job openings per year. The supply of graduates is substantially larger than the demand. Indeed, in surveys of recent computer science graduates, 32 percent of those graduates not entering the IT workforce say it is because IT jobs are unavailable, while 53 percent say they found better job opportunities outside of IT occupations.[19]

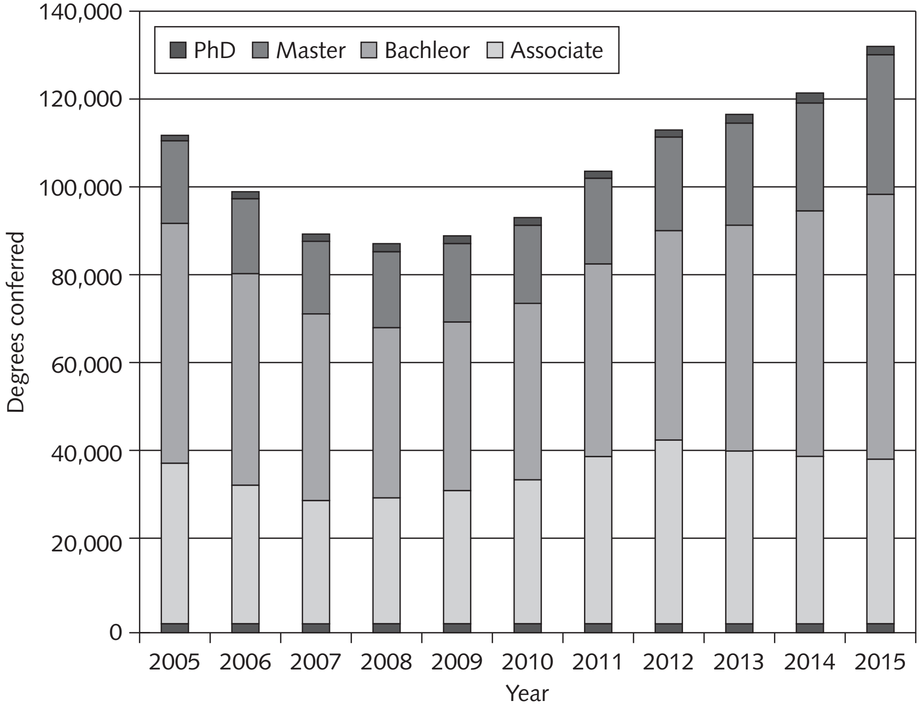


FIGURE 10-2 Number of computer and information science degrees granted by year

Source: "Digest of Education Statistics," National Center for Education Statistics

Opinions vary as to whether or not hiring of H-1B workers affects job opportunities and wages for U.S. workers. Many factors affect an individual's salary, including age, education, experience, citizenship status, race, sex, and employment location. Determining the impact of H-1B visas on employment opportunities and wages would require taking all these factors into account. However, the law of supply and demand makes clear that where the supply of workers exceeds the demand for workers for a specific job classification in a specific geographic area, one can expect unemployment and a decrease in salaries.

One recent study concluded that without H-1B visa workers, wages for U.S. computer scientists would have been 2.6 percent to 5.1 percent higher and employment in the computer science field for U.S. workers would have been 6.1 percent to 10.8 percent higher in 2001.[20] Critics of this study, however, point out that its conclusions are based on data nearly a decade old and that circumstances have changed.

Another study used salary data from 2016 for 10 large U.S. cities and found that when comparing workers in the same jobs, in the same cities, H-1B workers earn on average 2.8 percent more than their U.S. counterparts. Jobs where H-1B workers often earn more than U.S. workers include professor, program manager, project manager, and risk manager. Jobs where they typically earn less include data scientist, financial analyst, programmer analyst, and software engineer.[21]

CRITICAL THINKING EXERCISE: NEW H-1B WORKERS AT YOUR FIRM

You are having lunch in your company's cafeteria when two coworkers sit down to eat with you. The conversation turns to the latest company rumors, including discussion of the expected hiring of 10 H-1B workers to augment your current IT staff of 50 workers. Your coworkers are concerned that the new workers will lead to terminations among the existing IT staff and a freeze on salary increases for those remaining. What would you say?

OUTSOURCING

Outsourcing is another approach for meeting staffing needs. **Outsourcing** is a long-term business arrangement in which a company contracts for services with an outside organization that has expertise in providing a specific function. A company may contract with an organization to provide services such as operating a data center, supporting a telecommunications network, developing software, or staffing a computer help desk.

Stonewood Financial Tools, a privately held financial services company with headquarters in Louisville, Kentucky, provides investment tools that enable people to make well-informed financial decisions. Recently, Stonewood decided it wanted to develop a custom application that could recommend the best retirement income products for its clients based on a broad set of criteria. With fewer than 50 employees, Stonewood did not have sufficient software development expertise in-house, so it outsourced the work to GlowTouch, an outsourcing firm with 1,200 employees that provides small and mid-sized companies with fast, scalable, responsive IT services. Stonewood and GlowTouch worked together to define and implement an application that meets the needs and provides real-time retirement estimates to Stonewood's clients.[22]

Coemployment legal problems with outsourcing are minimal because the company that contracts for the services does not generally supervise or control the contractor's employees. The primary rationale for outsourcing is to lower costs, but companies also use it to obtain strategic flexibility and to keep their staff focused on the company's core competencies.

Offshore Outsourcing

Offshore outsourcing is a form of outsourcing in which services are provided by an organization whose employees are in a foreign country. Any work done at a relatively high cost in the United States may become a candidate for offshore outsourcing—not just IT work. However, IT professionals in particular can do much of their work anywhere—on a company's premises or thousands of miles away in a foreign country. In addition, companies can reap large financial benefits by reducing labor costs through offshore outsourcing. As a result, and because a large supply of experienced IT professionals is readily available in certain foreign countries, the use of offshore outsourcing in the IT field is common.

Outsourcing is not a recent phenomenon. Accenture, Cap Gemini, Hewlett Packard, and IBM have sent thousands of jobs offshore since the mid-1990s.[23] However, the use of offshore outsourcing has been declining in recent years. While 20 percent of leading tech firms employed offshore outsourcing in 2015, this was down from 27 percent in 2014 and 37 percent in 2013.[24]

Many U.S. software firms set up development centers in low-cost foreign countries where they have access to a large pool of well-trained candidates. Intuit—maker of the Quicken tax preparation software—currently has software development facilities in California and India. Accenture, IBM, and Microsoft all maintain large development centers in India. Cognizant Technology Solutions is headquartered in Teaneck, New Jersey, but operates primarily from technology centers in India.

Because of the high salaries earned by application developers in the United States and the ease with which customers and suppliers can communicate, it is now quite common to use offshore outsourcing for major programming projects. India, with its rich talent pool (a high percentage of whom speak English) and low labor costs, is considered one of the best sources of programming skills outside Europe and North America. Other sources of skilled contract programmers are China, Russia, Poland, Switzerland, and Hungary.[25]

Organizations must consider many factors when deciding where to locate outsourcing activities. For example, political unrest and violence in Egypt reduced the attractiveness of that country as a source of IT outsourcing, particularly after the government there temporarily blocked all Internet and cell phone service in early 2011.[26]

Table 10-7 lists the top IT outsourcing firms for 2016, according to the outsourcing consultancy and research firm Everest Group. The rankings are based on an evaluation of each company's performance in 26 different categories, including key business lines, geographies, and technologies, with a particular emphasis on innovation, intellectual property, and emerging technology capabilities.

TABLE 10-7 Top-rated IT outsourcing firms

Firm	Headquarters location
Cognizant Technology Solutions	Teaneck, New Jersey
Accenture	Dublin, Ireland
IBM	Armonk, New York
Tata Consulting Services	Mumbai, India
Wipro Technologies	Bangalore, India
HCL	Noida, India
Dell	Round Rock, Texas
Infosys Technologies	Bangalore, India
Capgemini+IGATE	Paris, France
CSC	Falls Church, Virginia

Source: Stephanie Overby, "The Top 10 IT Outsourcing Service Providers of the Year," CIO, February 8, 2016, www.cio.com/article/3030989/outsourcing/the-top-10-it-outsourcing-service-providers-of-the-year.html.

Pros and Cons of Offshore Outsourcing

Wages that an American worker might consider low represent an excellent salary in many other parts of the world, and some companies feel they would be foolish not to exploit such an opportunity. Why pay a U.S. IT worker a six-figure salary, they reason, when they can use offshore outsourcing to hire three India-based workers for the same cost? However, this attitude might represent a short-term point of view—offshore demand is driving up salaries in India by roughly 15 percent per year. Because of this, Indian offshore suppliers have begun to charge more for their services. The cost advantage for offshore outsourcing to India used to be 6:1 or more—you could hire six Indian IT workers for the cost of one U.S. IT worker. The cost advantage is shrinking, and once it reaches about 1.5:1, the cost savings will no longer be much of an incentive for U.S. offshore outsourcing to India.

Another benefit of offshore outsourcing is its potential to dramatically speed up software development efforts. For example, FirstBest Systems, a leading provider of insurance software solutions and services, contracted the integration and implementation of an underwriting management system to Syntel, one of the first U.S. firms to successfully launch a global delivery model that enables workers to work on a project around the clock.[27] With technical teams working from networked facilities in different time zones, Syntel executes a virtual "24-hour workday" that saves its customers money, speeds projects to completion, and provides continuous support for key software applications.

While offshore outsourcing can save a company in terms of labor costs, it will also result in other expenses. In determining how much money and time a company will save with offshore outsourcing, the firm must take into account the additional time that will be required to select an offshore vendor as well as the additional costs that will be incurred for travel and communications. In addition, organizations often find it takes years of ongoing effort and a large up-front investment to develop a good working relationship with an offshore outsourcing firm. Finding a reputable vendor can be especially difficult for a small or midsized firm that lacks experience in identifying and vetting contractors.

Many of the ethical issues that arise when considering whether to use H-1B and contingent workers also apply to outsourcing and offshore outsourcing. For example, managers must consider the trade-offs between using offshore outsourcing firms and devoting money and time to retain and develop their own staff. Often, companies that begin offshoring also lay off portions of their own staff as part of that move.

Cultural and language differences can cause misunderstandings among project members in different countries. For example, in some cultures, shaking one's head up and down simply means "Yes, I understand what you are saying." It does not necessarily mean "Yes, I agree with what you are saying." And the difficulty of communicating directly with people over long distances can make offshore outsourcing perilous, especially when key team members speak English as their second language.

The compromising of customer data is yet another potential outsourcing issue. In a study to understand the risks associated with services outsourcing, researchers at Arizona State University analyzed 146 customer data breaches between 2005 and 2010. Of those, 25 were breaches for which the outsourced service provider was responsible.[28] Clearly, organizations that outsource must take precautions to protect private data, regardless of where it is stored or processed.

Another downside to offshore outsourcing is that a company loses the knowledge and experience gained by outsourced workers when those workers are reassigned after a project's completion. Finally, offshore outsourcing does not advance the development of permanent IT workers in the United States, which increases its dependency on foreign workers to build the IT infrastructure of the future. Many of the jobs that go overseas are entry-level positions that help develop employees for future, more responsible positions.

Strategies for Successful Offshore Outsourcing

Successful projects require day-to-day interaction between software development and business teams, so it is essential for the hiring company to take a hands-on approach to project management. Companies cannot afford to outsource responsibility and accountability.

To improve the chances that an offshore outsourcing project will succeed, a company must carefully evaluate whether an outsourcing firm can provide the following:

- Employees with the required expertise in the technologies involved in the project
- A project manager who speaks the employer company's native language
- A pool of staff large enough to meet the needs of the project
- A reliable, state-of-the-art communications network
- High-quality, on-site managers and supervisors

To ensure that company data is protected in an outsourcing arrangement, companies can use the Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). A successful **SSAE No. 16 audit report** demonstrates that an outsourcing firm has effective internal controls in accordance with the Sarbanes-Oxley Act of 2002. The International Standard on Assurance Engagements **(ISAE) No. 3402**, Assurance Reports on Controls at a Service Organization, was issued by the International Auditing and Assurance Standards Board (IAASB) and is the international counterpart to SSAE No. 16.

The following list provides several tips for companies that are considering offshore outsourcing:

- Set clear, firm business specifications for the work to be done.
- Assess the probability of political upheavals or factors that might interfere with information flow, and ensure the risks are acceptable.
- Assess the basic stability and economic soundness of the outsourcing vendor and what might occur if the vendor encounters a severe financial downturn.
- Establish reliable satellite or broadband communications between your site and the outsourcer's location.
- Implement a formal version-control process, coordinated through a quality assurance person.
- Develop and use a dictionary of terms to encourage a common understanding of technical jargon.
- Require vendors to have project managers at the client site to overcome cultural barriers and facilitate communication with offshore programmers.
- Require a network manager at the vendor site to coordinate the logistics of using several communications providers around the world.
- Agree in advance on the structure and content of documentation to ensure that manuals explain how the system was built, as well as how to maintain it.
- Carefully review a current copy of the outsourcing firm's SSAE No. 16 or ISAE No. 3402 audit report to ascertain its level of control over information technology and related processes.

CRITICAL THINKING EXERCISE: PROS AND CONS OF OUTSOURCING

Your organization is about to embark on a major software development project that is expected to require a full-time project manager, an IT infrastructure architect, two Web developers, six software developers, two systems analysts, and a database administrator over a period of six-to-nine months. Your organization does not have the staff to complete this effort. Management is considering either outsourcing the effort to a U.S. software development firm with which they have had good success in the past or offshore outsourcing the project to Tata Consulting Services. Your organization has limited experience with offshore outsourcing, but management estimates that the total project cost could be reduced from around $3.0 million to less than $1.5 million by using Tata. What additional information do you need to make a fully informed decision about which option to execute? What are the pros and cons of each option?

WHISTLE-BLOWING

Whistle-blowing is an effort to attract public attention to a negligent, illegal, unethical, abusive, or dangerous act by an individual or organization. In some cases, whistle-blowers are employees who act as informants on their company, revealing information to enrich themselves or to gain revenge for a perceived wrong. In most cases, however, whistle-blowers act ethically in an attempt to correct what they think is a major wrongdoing, often at great personal risk.

A whistle-blower usually has personal knowledge of what is happening inside the offending organization because of his or her role as an employee of the organization. Sometimes the whistle-blower is not an employee but a person with special knowledge gained from a position as an auditor or business partner.

In going public with the information they have, whistle-blowers often risk their own careers and sometimes even affect the lives of their friends and family. In extreme situations, whistle-blowers must choose between protecting society and remaining silent.

A senior finance manager at Oracle alleged she was fired for refusing to follow what she thought were unlawful accounting practices designed to boost sales revenue figures for the IT company's software-as-a-service and cloud computing services. In a whistle-blower lawsuit filed against the company, the former Oracle employee claimed she was instructed to add millions of dollars of accruals for anticipated business that had not yet materialized. Oracle stock dropped almost 4 percent the day following the filing of the lawsuit.[29] Oracle countered that the employee had worked there for under a year and was fired because she failed to fulfill the responsibilities of her role. Furthermore, Oracle claimed that she had never raised any allegations about unlawful accounting practices internally. The lawsuit between the employee and Oracle was settled in February 2017 but no details were released.[30]

Protection for Whistle-Blowers

Whistle-blower protection laws allow employees to alert the proper authorities to employer actions that are unethical, illegal, or unsafe, or that violate specific public policies.

Unfortunately, no comprehensive federal law protects all whistle-blowers from retaliatory acts. Instead, numerous laws protect a certain class of specific whistle-blowing acts in various industries. To make things even more complicated, each law has different filing provisions, administrative and judicial remedies, and statutes of limitations (which set time limits for legal action). Thus, the first step in reviewing a whistle-blower's claim of retaliation is for an experienced attorney to analyze the various laws and determine if and how the employee is protected. Once that is known, the attorney can determine what procedures to follow in filing a claim.

From the whistle-blower's perspective, a short statute of limitations is a major weakness of many whistle-blower protection laws. Failure to comply with the statute of limitations is a favorite defense of firms accused of wrongdoing in whistle-blower cases.

The **False Claims Act**, also known as the Lincoln Law, was enacted during the U.S. Civil War to combat fraud by companies that sold supplies to the Union Army. War profiteers sometimes shipped boxes of sawdust instead of guns, for instance, and some swindled the Union Army into purchasing the same cavalry horses several times. When it was enacted, the act's goal was to entice whistle-blowers to come forward by offering them a share of the money recovered.

The **qui tam** ("who sues on behalf of the king as well as for himself") provision of the False Claims Act allows a private citizen to file a suit in the name of the U.S. government, charging fraud by government contractors and other entities who receive or use government funds. In qui tam actions, the government has the right to intervene and join the legal proceedings. If the government declines, the private plaintiff may proceed alone. Some states have passed similar laws concerning fraud in state government contracts.[31]

Qui tam actions can be based on a variety of charges, including mischarging for services, product and service substitution, false certification of entitlement for benefits, and false negotiation to justify an inflated contract. Mischarging is the most common charge in qui tam cases.[32] For example, an IT contractor might overcharge hundreds of hours of programming time as part of a government contract, or a physician might charge the government for medical services that a nurse actually performed.

Violators of the False Claims Act are liable for three times the dollar amount for which the government was defrauded. They can also be fined civil penalties of $5,000 to $10,000 for each instance of a false claim. A qui tam plaintiff can receive between 15 and 30 percent of the total recovery from the defendant, depending on how helpful the person was to the success of the case.[33]

The Department of Justice obtained more than $4.7 billion in settlements and judgments from civil cases involving fraud and false claims against the government in fiscal year 2016. Whistle-blowers filed 702 qui tam suits in fiscal year 2016. During the same period, the Department of Justice recovered $2.9 billion in connection with qui tam suits, while also awarding whistle-blowers close to $520 million.[34]

The False Claims Act provides strong whistle-blower protection. Any person who is discharged, demoted, harassed, or otherwise discriminated against because of lawful acts of whistle-blowing is entitled to all relief necessary "to make the employee whole." Such relief may include job reinstatement; double back pay; and compensation for any special damages, including litigation costs and reasonable attorney's fees.[35]

The provisions of the False Claims Act are complicated, so it is unwise to pursue a claim without legal counsel. However, because the potential for significant financial recovery is good, attorneys are generally willing to assist.

Whistle-Blowing Protection for Private-Sector Workers

Under state law, an employee could traditionally be terminated for any reason, or no reason, in the absence of an employment contract. However, many states have created laws that prevent workers from being fired because of an employee's participation in "protected" activities. One such activity is the filing of a qui tam lawsuit under the provisions of the False Claims Act. States that recognize the public benefit of such cases offer protection to whistle-blowers; for example, whistle-blowers may be able to file claims against their employers for retaliatory termination and may be entitled to a jury trial. If successful, they may receive punitive damage awards.

Dealing with a Whistle-Blowing Situation

Each potential whistle-blowing case involves different circumstances, issues, and personalities. Two people working together in the same company may have different values and concerns that cause them to react in different ways to a particular situation—and both reactions might be ethical. It is impossible to outline a definitive step-by-step procedure of how to behave in a whistle-blowing situation. This section provides a general sequence of events and highlights key issues that a potential whistle-blower should consider. Anyone considering becoming a whistle-blower is strongly advised to seek legal counsel.

Assess the Seriousness of the Situation

Before considering whistle-blowing, a person should have specific knowledge that his or her company or a coworker is acting unethically and that the action represents a *serious* threat to the public interest. The employee should carefully and informally seek trusted resources outside the company and ask for their assessment. Do they also see the situation as serious? Their point of view may help the employee see the situation from a different perspective and alleviate concerns. On the other hand, the outside resources may reinforce the employee's initial suspicions, forcing a series of difficult ethical decisions.

Begin Documentation

An employee who identifies an illegal or unethical practice should begin to compile adequate documentation to establish wrongdoing. The documentation should record all events and facts as well as the employee's insights about the situation. This record helps construct a chronology of events if legal testimony is required in the future. An employee should identify and copy all supporting memos, correspondence, manuals, and other documents *before* taking the next step. Otherwise, records may disappear and become inaccessible. The employee should maintain documentation and keep it up to date throughout the process.

Attempt to Address the Situation Internally

An employee should next attempt to address the problem internally by providing a written summary to the appropriate managers. Ideally, the employee can expose the problem and deal with it from inside the organization. The focus should be on disclosing the facts and how the situation affects others. The employee's goal should be to fix the problem, not to place blame. Given the potential negative impact of whistle-blowing on the employee's future, this step should not be dismissed or taken lightly.

Fortunately, many problems are solved at this point, and further, more drastic actions by the employee are unnecessary. The appropriate managers get involved and resolve the issue that initiated the whistle-blower's action.

On the other hand, managers who are engaged in unethical or illegal behavior might not welcome an employee's questions or concerns. In such cases, the whistle-blower can expect to be strongly discouraged from taking further action. Employee demotion or termination on false or exaggerated claims can occur. Attempts at discrediting the employee can also be expected. As an extreme example, Dr. Jeffrey Wigand, former vice president of research and development at Brown & Williamson, disclosed wrongdoings involving the use of cancer-causing ingredients in the tobacco industry. As a result, he received several anonymous death threats; however, none of the threats could be traced back to its source.[36]

Consider Escalating the Situation Within the Company

The employee's initial attempt to deal with a situation internally may be unsuccessful. At this point, the employee may rationalize that he or she has done all that is required by raising the issue. Others may feel so strongly about the situation that they are compelled to take further action. Thus, a determined and conscientious employee may feel forced to choose between escalating the problem and going over the manager's head, or going outside the organization to deal with the problem. The employee may feel obligated to sound the alarm on the company because there appears to be no chance to solve the problem internally.

Going over an immediate manager's head can put one's career in jeopardy. Supervisors may retaliate against a challenge to their management, although some organizations may have an effective corporate ethics officer who can be trusted to give the employee a fair and objective hearing. Alternatively, a senior manager with a reputation for fairness and some responsibility for the area of concern might step in. However, in many work environments, the challenger may be fired, demoted, or reassigned to a less desirable position or job location. Such actions send a loud signal throughout an organization that loyalty is highly valued and that challengers will be dealt with harshly. Whether reprisal is ethical depends in large part on the legitimacy of the employee's issue. If the employee is truly overreacting to a minor issue, then the employee may deserve some sort of reprimand for exercising poor judgment.

If senior managers refuse to deal with a legitimate problem, the employee can decide to drop the matter or go outside the organization to try to remedy the situation. Even if a senior manager agrees with the employee's position and overrules the employee's immediate supervisor, the employee may want to request a transfer to avoid working for the same person.

Assess the Implications of Becoming a Whistle-Blower

If whistle-blowers feel they have made a strong attempt to resolve the problem internally without results, they must stop and fully assess whether they are prepared to go forward and blow the whistle on the company. Depending on the situation, an employee may incur significant legal fees in order to bring charges against an agency or company that may have access to an array of legal resources as well as a lot more money than the individual employee. An employee who chooses to proceed might be accused of having a grievance with the employer or of trying to profit from the accusations. The employee may be fired and may lose the confidence of coworkers, friends, and even family members. A potential whistle-blower must attempt to answer many ethical questions before making a decision on how to proceed:

- Given the potentially high price, do I really want to proceed?
- Have I exhausted all means of dealing with the problem? Is whistle-blowing all that is left?
- Am I violating an obligation to be loyal to my employer and work for its best interests?
- Will the public exposure of corruption and mismanagement in the organization really correct the underlying cause of these problems and protect others from harm?

From the moment an employee becomes known as a whistle-blower, a public battle may ensue. Whistle-blowers can expect attacks on their personal integrity and character as well as negative publicity in the media. Friends and family members will hear these accusations, and ideally, they should be notified beforehand and consulted for advice before the whistle-blower goes public. This notification helps prevent friends and family members from being surprised at future actions by the whistle-blower or the employer.

The whistle-blower should also consider consulting support groups, elected officials, and professional organizations. For example, the National Whistleblowers Center provides referrals for legal counseling and education about the rights of whistle-blowers.

Use Experienced Resources to Develop an Action Plan

A whistle-blower should consult with competent legal counsel who has experience in whistle-blowing cases. He or she will determine which statutes and laws apply, depending on the agency, the employer, the state involved, and on the nature of the case. Counsel should also know the statute of limitations for reporting the offense, as well as the whistle-blower's protection under the law. Before blowing the whistle publicly, the employee should get an honest assessment of the soundness of his or her legal position and an estimate of the costs of a lawsuit.

Execute the Action Plan

A whistle-blower who chooses to pursue a matter legally should do so based on the research and guidance of legal counsel. If the whistle-blower wants to remain unknown, the safest course of action is to leak information anonymously to the press. The problem with this approach, however, is that anonymous claims are often not taken seriously. In most cases, working directly with appropriate regulatory agencies and legal authorities is more likely to get results, including the imposition of fines, the halting of operations, or other actions that draw the offending organization's immediate attention.

Live with the Consequences

Whistle-blowers must be on guard against retaliation, such as being discredited by coworkers, threatened, or set up; for example, management may attempt to have the whistle-blower transferred, demoted, or fired for breaking some minor rule, such as arriving late to work or leaving early. To justify their actions, management may argue that such behavior has been ongoing. The whistle-blower might need a good strategy and a good attorney to counteract such actions and take recourse under the law.

A massive computer-data breach at TJX (the parent company of T.J. Maxx, Marshalls, and other stores) affecting 94 million Visa and MasterCard accounts occurred in June 2005.[37] A college student who was an hourly worker at TJX noticed many computer-related security problems at the firm prior to the data breach. He reported these verbally to TJX managers and also posted information about the breaches on an online security forum. In the forum, he revealed serious security weaknesses with sufficient detail that the information could be of use to hackers. The employee spoke to store managers and the district loss prevention manager before the data breach occurred, but nothing was done. Eventually the worker was fired over the public disclosures and violation of his nondisclosure agreement.[38] This is a perfect example of how *not* to be a whistle-blower.

CRITICAL THINKING EXERCISE: WHISTLE-BLOWER SITUATION?

You graduated from a local nursing school with a bachelor of science degree in nursing, and you have seven years of experience working at three different hospitals. Recently, you were promoted to charge nurse, responsible for the operation of the nursing unit during the 7 p.m. to 7 a.m. shift. You are well respected by the other nurses and physicians for your excellent management skills and sound decision making. As a result, you were assigned to be a member of a group of seven individuals who are evaluating options to replace the hospital's aging IT infrastructure—laptops, tablets, data storage systems, and network devices. While you have limited IT expertise, you are responsible for representing the end user needs and ensuring that whatever vendors and equipment are selected, it will all work together reliably and efficiently. Other members of the team come from the IT and finance organizations.

The other members of this project have converged on a set of vendors and equipment. Their choice is based mainly on obtaining "state-of-the-art" technology with tremendous data processing speed and capacity that will allow for anticipated growth in the number of patients to be served. However, when you talk to employees at other hospitals that have implemented the same solution, they are highly dissatisfied due to poor system reliability and availability. Many report there have been system outages of several hours multiple times during the last year.

In the latest project team meeting, a poll was taken and the vote was 6-1 in favor of the state-of-the-art solution. You were the sole dissenting vote. The project manager stated that he will proceed in finalizing contracts (totaling some $6 million) and preparing a schedule for implementation.

You are greatly concerned that the project team is about to make a serious mistake, but you seem unable to affect their decision. Is this a potential whistle-blowing situation? How should you proceed?

GREEN COMPUTING

Electronic devices such as computers and smartphones contain hundreds—or even thousands—of components, which are, in turn, composed of many different materials, including some (such as beryllium, cadmium, lead, mercury, brominated flame retardants

(BFRs), selenium, and polyvinyl chloride) that are known to be potentially harmful to humans and the environment.[39] Electronics manufacturing employees and suppliers at all steps along the supply chain and manufacturing process are at risk of unhealthy exposure to these raw materials. Users of these products can also be exposed to these materials when using poorly designed or improperly manufactured devices. Care must also be taken when recycling or destroying these devices to avoid contaminating the environment.

Green computing is concerned with the efficient and environmentally responsible design, manufacture, operation, and disposal of IT-related products, including all types of computing devices (from smartphones to supercomputers), printers, printer materials such as cartridges and toner, and storage devices. Green computing has three goals: (1) reduce the use of hazardous material, (2) allow companies to lower their power-related costs, and (3) enable the safe disposal or recycling of computers and computer-related equipment. Many business organizations recognize that going green is in their best interests in terms of public relations, employee safety, and the community at large. These organizations also recognize that green computing presents an opportunity to substantially reduce total costs over the life cycle of their IT equipment.

It is estimated that in the United States, 51.9 million computers, 35.8 million monitors, and 33.6 million hard copy devices (printers, faxes, etc.)—representing a total of 1.3 million tons of waste—were disposed of in 2010 alone.[40] E-waste is the fastest growing municipal waste stream in the United States, according to the EPA. Because it is impossible for manufacturers to ensure safe recycling or disposal, the best practice would be for them to eliminate the use of toxic substances, particularly since recycling of used computers, monitors, and printers has raised concerns about toxicity and carcinogenicity of some of the substances. However, until manufacturers stop using these toxic substances, safe disposal and reclamation operations must be carried out carefully to avoid exposure in recycling operations and leaching of materials, such as heavy metals, from landfills and incinerator ashes. In many cases, recycling companies export large quantities of used electronics to companies in undeveloped countries. Unfortunately, many of these countries do not have strong environmental laws, and they sometimes fail to recognize the potential dangers of dealing with hazardous materials. In their defense, these countries point out that the United States and other first-world countries were allowed to develop robust economies and rise up out of poverty without the restrictions of strict environmental policies.

Electronic Product Environmental Assessment Tool (EPEAT) is a system that enables purchasers to evaluate, compare, and select electronic products based on a total of 51 environmental criteria. Products are ranked in EPEAT according to three tiers of environmental performance: Bronze (meets all 23 required criteria), Silver (meets all 23 of the required criteria plus at least 50 percent of the optional criteria), and Gold (meets all 23 required criteria plus at least 75 percent of the optional criteria), as shown in Table 10.8. EPEAT was first implemented in 2006 with Computer and Displays (IEEE 1680.1 standard) and has now expanded to Imaging Equipment, under the IEEE 1680.2 standard from January 2013. EPEAT is managed by the Green Electronics Council and currently evaluates more than 4,400 products from more than 60 manufacturers across 43 countries.[41]

TABLE 10-8 EPEAT product tiers for computers

Tier	Number of required criteria that must be met	Number of optional criteria that must be met
Bronze	All 23	None
Silver	All 23	At least 50%
Gold	All 23	At least 75%

Source: "EPEAT Criteria," EPEAT, June 23, 2011, www.epeat.net/resources/criteria-2/, accessed May 31, 2017.

Individual purchasers as well as corporate purchasers of computers, printers, scanners, and multifunction devices can use the EPEAT website (www.epeat.net) to screen manufacturers and models based on environmental attributes.[42] Since 2007, U.S. Federal agency purchasers have been directed to meet an annual commitment of 95 percent or higher EPEAT purchasing in all covered product categories, first by Presidential Executive Order and then by regulatory requirement.[43]

The European Union's Restriction of Hazardous Substances Directive, which took effect in 2006, restricts the use of many hazardous materials in computer manufacturing. The directive also requires manufacturers to use at least 65 percent reusable or recyclable components, implement a plan to manage products at the end of their life cycle in an environmentally safe manner, and reduce or eliminate toxic material in their packaging. The state of California has passed a similar law, called the Electronic Waste Recycling Act. Because of these two acts, manufacturers had a strong motivation to remove brominated flame retardants from their PC casings. By the start of 2010, the Apple iPad was free of arsenic, mercury, PVC (polyvinyl chloride), and BFRs. In addition, according to Apple, the iPad's aluminum and glass enclosure is "highly recyclable."[44]

Lenovo is a Chinese manufacturer of personal computers, tablets, smartphones, workstations, servers, electronic storage devices, and printers. Since 2007, the company's product development teams have been using increasing amounts of recycled plastics to meet new customer requirements, satisfy corporate environmental objectives and targets, and achieve EPEAT Gold registrations for its products. The company's efforts have resulted in the avoidance of up to 248 million pounds of CO2 emissions since 2007.[45]

CRITICAL THINKING EXERCISE: MOVING TO GREEN COMPUTING

Your organization is a leader in the development of renewable energy sources based on enhanced geothermal systems and is viewed as a champion in the fight to reduce carbon emissions. The organization employs over 25,000 people worldwide and operates three global data centers, one each in the United States, Europe, and Southeast Asia. The CEO has asked all her direct reports for input on a proposed strategy to become a leader in green computing. In what ways is a move toward green computing consistent with your organization's mission of developing renewable energy sources? One green computing proposal is to consolidate the three data centers into one. Discuss the pros and cons of this approach. Can you identify any other tactics the organization might take to accelerate its move toward green computing? Identify the pros and cons or any issues associated with your proposed tactics.

Summary

What key legal and ethical issues are associated with the use of contingent workers, H-1B visa holders, and offshore outsourcing companies?

- Contingent work is a job situation in which an individual does not have an explicit or implicit contract for long-term employment.
- Organizations can obtain contingent workers through temporary staffing firms, employee leasing organizations, and professional employment organizations.
- Temporary staffing firms recruit, train, and test job seekers in a wide range of job categories and skill levels, and then assign them to clients as needed.
- In employee leasing, the subscribing firm transfers all or part of its workforce to the leasing firm, which handles all human-resource-related activities and costs such as payroll, training, and the administration of employee benefits. The subscribing firm leases these workers, but they remain employees of the leasing firm.
- A coemployment relationship is one in which two employers have actual or potential legal rights and duties with respect to the same employee or group of employees.
- A PEO is a business entity that hires the employees of its clients and then assumes all responsibility for all human resource management functions, including administration of benefits. The client company remains responsible for directing and controlling the daily activities of the employees. The client maintains a long-term investment and commitment to the employees, but uses the PEO as a means to outsource the human resource activities.
- The gig economy refers to a work environment in which temporary positions are common and organizations contract with independent workers for short-term engagements.
- An independent contractor is an individual who provides services to another individual or organization according to terms defined in a written contract or within a verbal agreement.
- Organizations that use contingent workers must be extremely careful how they pay and treat these workers, or run the risk of getting dragged into a class action lawsuit over misclassification of workers.
- When a firm employs a contingent worker, it does not usually have to provide benefits, can easily adjust the number of workers to meet its business needs, and does not incur training costs.
- Contingent workers may have a low level of commitment to the company and its projects. The skills and knowledge a contingent worker gains while working for a particular are lost when the worker departs at a project's completion.
- An H-1B is a temporary work visa granted by the U.S. Citizenship and Immigration Services (USCIS) for people who work in specialty occupations—jobs that require at least a four-year bachelor's degree in a specific field, or equivalent experience.
- Employers hire H-1B workers to meet critical business needs or to obtain essential technical skills or knowledge that cannot be readily found in the United States. H-1B workers may also be used when there are temporary shortages of needed skills.
- Congress sets an annual cap on the number of H-1B visas to be granted—although the number of visas issued often varies greatly from this cap due to various exceptions.

- Companies applying for H-1B visas must offer a wage that is at least 95 percent of the average salary for the occupation. Because wages in the IT field vary substantially, unethical companies can get around the average salary requirement.
- Companies that employ H-1B workers are required to declare that they will not displace American workers; however, they are exempt from that requirement if 15 percent of more of their workers are on H-1B visas and the H-1B workers are paid at least $60,000 a year.
- Many U.S. companies complain they have trouble finding enough qualified workers and urge that the cap on visas be raised. Unemployed and displaced IT workers challenge whether the United States needs to continue importing tens of thousands of H-1B workers each year.
- The number of degrees awarded in the field of computer and information sciences at post-secondary institutions in the United States reached 130,000 in 2015. The Bureau of Labor Statistics has projected an increase of 53,000 new U.S. tech jobs per year from 2014 to 2024.
- Opinions vary as to whether or not the hiring of H-1B workers affects job opportunities and wages.
- Outsourcing is a long-term business arrangement in which a company contracts for services with an outside organization that has expertise in providing a specific function.
- Offshore outsourcing is a form of outsourcing in which the services are provided by an organization whose employees are in a foreign country.
- Outsourcing and offshore outsourcing are used to meet staffing needs while potentially reducing costs and speeding up project schedules.
- Many of the same ethical issues that arise when considering whether to hire H-1B and contingent workers apply to outsourcing and offshore outsourcing.
- Successful offshoring projects require day-to-day interaction between software development and business teams, so it is essential for the hiring company to take a hands-on approach to project management.

What is whistle-blowing, and what ethical issues are associated with it?

- Whistle-blowing is an effort to attract public attention to a negligent, illegal, unethical, abusive, or dangerous act by a company or some other organization.
- Whistle-blower protection laws allow employees to alert the proper authorities to employer actions that are unethical, illegal, or unsafe, or that violate specific public policies. Unfortunately, no comprehensive federal law protects all whistle-blowers from retaliatory acts.
- A potential whistle-blower must consider many ethical implications prior to going public with his or her allegations, including whether the high price of whistle-blowing is worth it; whether all other means of dealing with the problem have been exhausted; whether whistle-blowing violates the obligation of loyalty that the employee owes to his or her employer; and whether public exposure of the problem will actually correct its underlying cause and protect others from harm.
- An effective whistle-blowing process includes the following steps: (1) assess the seriousness of the situation, (2) begin documentation, (3) attempt to address the situation internally, (4) consider escalating the situation within the company, (5) assess the implications

of becoming a whistle-blower, (6) use experienced resources to develop an action plan, (7) execute the action plan, and (8) live with the consequences.

What is green computing, and what are organizations doing to support this initiative?

- Green computing is concerned with the efficient and environmentally responsible design, manufacture, operation, and disposal of IT-related products.
- Green computing has three goals: (1) reduce the use of hazardous material, (2) allow companies to lower their power-related costs, and (3) enable the safe disposal or recycling of computers and computer-related equipment.
- Electronic Product Environmental Assessment Tool (EPEAT) is a system that enables purchasers to evaluate, compare, and select electronic products based on 51 environmental criteria.
- The European Union passed the Restriction of Hazardous Substances Directive to restrict the use of many hazardous materials in computer manufacturing, require manufacturers to use at least 65 percent reusable or recyclable components, implement a plan to manage products at the end of their life cycle in an environmentally safe manner, and reduce or eliminate toxic material in their packaging.

Key Terms

coemployment relationship

contingent work

employee leasing

Electronic Product Environmental Assessment Tool (EPEAT)

False Claims Act

gig economy

green computing

H-1B visa

independent contractor

ISAE No. 3402

offshore outsourcing

outsourcing

professional employer organization (PEO)

qui tam

SSAE No. 16 audit report

whistle-blowing

Self-Assessment Questions

What key legal and ethical issues are associated with the use of contingent workers, H-1B visa holders, and offshore outsourcing companies?

1. A ______________ hires the employees of its clients and then assumes responsibility for all human resource functions. If this arrangement is terminated, the workers continue to be employed by the client company.
   a. temporary staffing firm
   b. professional employer organization (PEO)
   c. employee leasing firm
   d. temporary employment agency

2. ______________ is one in which two employers have legal rights and duties with respect to the same employee or group of employees.

3. Which of the following is *not* an advantage for organizations that employ contingent workers?
   a. The company can release contingent workers when they are no longer needed.
   b. Training costs are kept to a minimum.
   c. Contingent workers provide a way to meet fluctuating staffing needs.
   d. The contingent worker's experience may be useful to the next firm that hires him or her.

4. Which of the following statements indicate that the worker is not an independent contractor?
   a. No federal income tax, Social Security tax, or Medicare taxes are withheld from his paycheck.
   b. The worker is protected by workplace safety and employment antidiscrimination laws.
   c. He is not eligible for unemployment compensation benefits.
   d. The worker sets his own work hours.

5. The National Labor Relations Act, Civil Rights Act, Air Labor Standards, and Employee Retirement Income Security Act each all have a uniform, consistent definition of employee and the same way of distinguishing between employees and independent contractors. True or False?

6. The top country of birth for H-1B workers in the United States in 2015 was
   a. Canada
   b. Mexico
   c. China
   d. India

7. Which group of foreign workers is not exempt from the annual cap on the number of H-1B visas granted?
   a. Scientists hired to teach at U.S. universities.
   b. Those hired to work in government research labs.
   c. Those hired to work in nonprofit organizations.
   d. Programmers and engineers hired to work at private technology companies.

8. Which of the following statements is *not* true?
   a. All companies that employ H-1B workers are required to offer a wage not less than 95 percent of the average salary for the occupation.
   b. Congress sets an annual cap on the number of H-1B visas to be granted—although the number of visas issued often varies greatly from this cap due to various exceptions.
   c. Companies cannot use an H-1B worker classified as an entry-level IT employee to fill the position of a higher paid experienced worker.
   d. Companies with 15 percent or more of their workers on H-1B visas can use those workers to replace U.S. workers if those workers are paid at least $60,000 per year.

9. It appears that the current supply of U.S. computer and information science graduates exceeds the long-term BLS forecast of new job openings. True or False?

10. Coemployment legal problems with offshore outsourcing are minimal because ________.
    a. the primary rational for outsourcing is to lower costs
    b. the company that contracts for the services does not generally supervise or control the contractor's employees
    c. the services are provided by an organization whose employees are in a foreign country
    d. the IT professionals involved can do their work anywhere—on a company's premises or thousands of miles away

11. Which of the following statements about the offshore outsourcing of a major IT project is *not* true?
    a. It advances the development of permanent IT workers in the United States.
    b. There are likely additional costs associated with selection of a vendor, communications, and travel.
    c. Managers must make trade-offs between using offshore outsourcing firms and devoting time and money to retain and develop their own staff.
    d. Cultural and language differences can cause misunderstandings.

What is whistle-blowing, and what ethical issues are associated with it?

12. Which of the following statements about whistle-blowing is true?
    a. Violators of the False Claim Act are liable for four times the dollar amount that the government is defrauded.
    b. From the moment an employee becomes known as a whistle-blower, a public battle may ensue, with negative publicity attacks on the individual's personal integrity.
    c. Whistle-blowing is an effective approach to take in dealing with all work-related matters, from the serious to mundane.
    d. A whistle-blower must be an employee of the company that is the source of the problem.

13. No comprehensive federal law protects all whistle-blowers from retaliatory acts. True or False?

What is green computing, and what are organizations doing to support this initiative?

14. Electronic devices consist of many different materials, including some that are known to be harmful to humans and the environment. Which of the following groups of people are at risk of unhealthy exposure to these raw materials?
    a. Electronic manufacturing employees and suppliers at all steps along the supply chain.
    b. Users of these products when they are poorly designed or improperly manufactured.
    c. Residents near recycling plants.
    d. All of the above.

15. Which of the following statements about the European Union's Restriction of Hazardous Substances Directive is *not* true?
    a. It requires manufacturers to use at least 65 percent reusable or recyclable components.
    b. It requires manufacturers to implement a plan to manage products at the end of their life cycle in an environmentally safe manner.
    c. It enables purchasers to evaluate, compare, and select electronic products based on a total of 51 environmental criteria.
    d. It requires manufacturers to reduce or eliminate toxic material in their packaging.

Self-Assessment Answers

1. b; 2. coemployment relationship; 3. d; 4. b; 5. False; 6. d; 7. d; 8. c; 9. True; 10. b; 11.a; 12. b; 13. True; 14. d; 15. c

Discussion Questions

1. Briefly summarize the similarities and differences among temporary staffing firms, employee leasing organizations, and professional employment organizations. Which approach provides an organization the most protection from potential coemployment situations?
2. What steps must an organization take to ensure that someone they hired as an independent contractor cannot be considered an employee? Why is this important?
3. What are the advantages and disadvantages of using contingent workers?
4. Some people feel that it is unethical to hire H-1B workers to work in the United States. Prepare a brief summary of reasons why hiring H-1B workers might be considered unethical. Make a list of reasons why hiring H-1B workers should be considered an effective management strategy. Which set of reasons is stronger? Why?
5. How are unethical organizations gaming the H-1B visa program?
6. Do you feel that there is a shortage of experienced computer and information science graduates? Why or why not?
7. What factors must a company consider in deciding whether to employ offshore outsourcing on a project?
8. Do research to learn more about the SSAE No. 16 audit report—how is it used, what are its key elements, the different types of reports, and does it have any shortcomings? Write a one-page memo summarizing your findings.
9. While labor savings associated with offshore outsourcing may look attractive, what cost increases and other problems might one expect with such projects?
10. Your company has decided to offshore outsource a $50 million project to an experienced, reputable firm in India. This is the first offshore outsourcing project of significant size that your company has run. What steps should your company take to minimize the potential for problems?
11. Edward Snowden, a former employee of defense contractor Booz Allen Hamilton working at the National Security Agency (NSA), was responsible for perhaps the most significant leak of classified information in U.S. history. In June 2013, Snowden admitted to passing

classified documents to reporters at *The Guardian* and *The Washington Post*—revealing details of NSA surveillance programs that collect data and perform data mining on hundreds of millions of U.S. phone and Internet traffic records to identify possible links to known terrorists. Shortly after leaking the documents, Snowden fled the country to avoid federal charges. Some people call Snowden a whistle-blower for drawing attention to NSA programs they feel violate civil rights and the Constitution. Others consider him a traitor and feel he should be heavily prosecuted. Do further research on this incident and write a one-page report providing your point of view.

12. Briefly describe a situation that could occur at your employer or your school that would rise to the level of a potential whistle-blower situation. What steps would you take and to whom would you speak to call this matter to the attention of appropriate members of management?
13. How would you define green computing? What are its goals?
14. Visit the EPEAT website (www.epeat.net), and use the organization's tool to select your next laptop or tablet computer. How would you make trade-offs between an expensive machine with a Gold rating and a less expensive machine with the same features and performance but only a Bronze rating?

What Would You Do?

Use the five-step decision-making process discussed in Chapter 1 to analyze the following situations and recommend a course of action.

1. Your firm has just added six H-1B workers to your 50-person department. You have been asked to help get one of the workers "on board." Your manager wants you to introduce him to other team members, provide him with some basic company background and information, and explain to him how work gets done within your organization. Your manager has also asked that you help your new coworker become familiar with the community, including residential areas, shopping centers, restaurants, and recreational activities. Your goal would be to help the new worker be productive and comfortable with his new surroundings as soon as possible. How would you feel about taking on this responsibility? How would you go about doing this?
2. As a relatively new hire within a large multinational firm, you are extremely pleased with the many challenging assignments that have come your way. Now another new hire with whom you have become friends is seeking your input on an important decision that she must make within the next week. She has been told that the firm has decided to cut costs in her department by outsourcing a large portion of the department's work to an offshore resource firm that has an excellent reputation. Your friend would remain with the firm to oversee the transition of work to the outsourcing firm including training the new workers, establishing performance benchmarks and measures, tracking results, and providing ongoing feedback to management both at your firm and the outsourcing firm. She is very concerned that there will be great tension as some 25 workers are replaced and feels that some of their anger will be directed at her. She is also concerned that once the start-up issues are resolved and things are running smoothly, she will be let go. What advice would you offer your friend?
3. A coworker complains to you that he is sick of seeing the manufacturing company where you are both employed pollute the waters of a nearby stream by dumping runoff water into

it from the manufacturing process. He plans to send an anonymous email to the EPA to inform the agency of the situation. What would you say to your coworker?

4. Dr. Jeffrey Wigand is a whistle-blower who was fired from his position of vice president of research and development at Brown & Williamson Tobacco Corporation in 1993. He was interviewed for a segment of the CBS show *60 Minutes* in August 1995, but the network made a highly controversial decision not to air the interview as initially scheduled. The segment was pulled because CBS management was worried about the possibility of a multibillion-dollar lawsuit for tortuous interference; that is, interfering with Wigand's confidentiality agreement with Brown & Williamson. The interview finally aired on February 4, 1996, after the *Wall Street Journal* published a confidential November 1995 deposition that Wigand gave in a Mississippi case against the tobacco industry, which repeated many of the charges he made to CBS. In the interview, Wigand said that Brown & Williamson had scrapped plans to make a safer cigarette and continued to use a flavoring in pipe tobacco that was known to cause cancer in laboratory animals. Wigand also charged that tobacco industry executives testified untruthfully before Congress about tobacco product safety. Wigand suffered greatly for his actions; he lost his job, his home, his family, and his friends.

   Visit Wigand's website at www.jeffreywigand.com and answer the following questions. (You may also want to watch *The Insider*, a 1999 movie based on Wigand's experience.)

   - What motivated Wigand to take an executive position at a tobacco company and then five years later to denounce the industry's efforts to minimize the health and safety issues of tobacco use?
   - What whistle-blower actions did Dr. Wigand take?
   - If you were in Dr. Wigand's position, what would you have done?

5. You are in the last stages of evaluating laptop vendors for a major hardware upgrade and standardization project for your firm. You will be purchasing a total of 800 new laptops and tablets to deploy to the worldwide sales force. One vendor's product carries a Bronze EPEAT rating; the other vendor's product would cost an additional $96,000 but carries a Gold EPEAT rating. The two products are very evenly matched on other key factors, such as performance, features, reliability, and support costs. How would you decide between the two vendors' products?

Cases

1. Disney Workers Replaced with H-1B Visa Workers

When some 250 IT workers at Walt Disney Parks and Resorts were laid off in 2015, a condition of their severance pay required some of them to train their replacements—workers from India who were in the United States on H-1B visas. Two of the displaced workers filed class action suits claiming that HCL and Cognizant Technology Solutions colluded with Disney to make false statements on certain forms when petitioning for workers to receive H-1B status. The suit alleged that those false statements were violations of the civil Racketeer Influenced and Corrupt Organizations (RICO) Act.

HCL and Cognizant are consulting firms that import workers to the United States on H-1B visas and then contract them out to U.S. firms. HCL is an India-based IT services company with 116,000 employees and annual revenue of $7 billion. Cognizant is a U.S.-based professional services company with annual revenue of $13 billion and over 260,000 employees (75 percent of whom are employed in India).

The Immigration and Nationality Act sets forth certain prerequisites for employers wishing to employ H-1B workers in the United States. To obtain H-1B status approval, the employer must first file a Labor Condition Application (LCA), Form ETA 9035 with the Department of Labor. The employer must state that it will: (1) pay the nonimmigrant workers at least the local prevailing wage or the employer's actual wage, whichever is higher; (2) pay for nonproductive time in certain circumstances; (3) offer benefits on the same basis as for U.S. workers; and (4) provide working conditions for H-1B workers that will not adversely affect the working conditions of workers similarly employed.

The civil RICO claims against HCL and Cognizant in the Disney case were based on the allegation that the two consulting firms engaged in racketeering activity by falsely stating on required Labor Department forms that the hiring of the nonimmigrant H-1B employees would not adversely affect the working conditions of workers similarly employed.

The U.S. District judge presiding over the case concluded that the facts failed to substantiate the RICO claim because declarations that the employment of H-1B workers would not adversely impact its U.S. workers did not pertain to Disney employees but rather to employees of HCL. In addition, a certification that H-1B employees would not displace American workers does not apply to so-called exempt H-1B workers who are paid at least $60,000 a year and possess certain education or skill levels. The judge dismissed the case, stating that HCL's statements weren't false, and would only have been false if HCL's own workers were adversely affected by the visa program.

Critical Thinking Questions

1. Does this case illustrate the need to make changes in the processing and approval of H-1B visas? If so, what changes do you think need to be made?
2. Do research to learn how effective this staffing solution turned out—is Disney happy with the results?
3. In April 2017, President Trump signed an Executive Order directing the government to review its policies on the H-1B visa program in an attempt to reduce any abuses of the program. Do research to identify any specific recommendations made to modify the H-1B visa program since this Executive Order was signed. What has been the impact or what might the impact of these changes be?

Sources: Claire Zillman, "Disney Lawsuit Reveals an H-1B Visa System That Heavily Favors Outsourcing Companies," *Fortune*, January 26, 2016, http://fortune.com/2016/01/26/disney-lawsuit-reveals-an-h-1b-visa-system-that-heavily-favors-large-outsourcing-companies/; Paul Brinkman, "Orlando Judge Tosses Disney IT Outsourcing Lawsuit," *Orlando Sentinel*, October 14, 2016, www.orlandosentinel.com/business/brinkmann-on-business/os-disney-visa-lawsuit-dismissed-20161014-story.html; "Federal Judge Says Disney Didn't Violate Visa Laws in Layoffs," *Watertown Daily News*, October 14, 2016, www.watertowndailytimes.com/national/federal-judge-says-disney-didnt-violate-visa-laws-in-layoffs-20161014; Scott M. Witch, "Court Upholds Disney's IT Outsourcing," *Society for Human Resource Management*, December 1, 2016, https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/disney-it-outsourcing.aspx; Nathan Hale, "Disney, Consulting Firms Dodge Worker Visa Abuse Claims," *Law360*, October 16, 2016, https://www.law360.com/articles/851258/disney-consulting-firms-dodge-worker-visa-abuse-claims; Te Rija Simhan, "Lay Off Threat for Over 6,000 at Cognizant Tech," *The Hindu Business Line*, March 18, 2017, www.thehindubusinessline.com/info-tech/cognizant-likely-to-lay-off-6000-employees/article9591070.ece.

Case 2: E-Waste—An Important Global Environmental and Health Issue

E-waste describes discarded electronic and IT devices destined for reuse, resale, salvage, recycling, or disposal. Over 46 million tons of e-waste are produced globally each year, and the toxic and complex minerals contained in e-waste can harm people's health and the environment when absorbed into the soil or water. Improper processing of e-waste (whether it is recycled or destroyed) can lead to adverse human health effects and environmental pollution.

There is money to be made in recycling e-waste to recover precious metals. For example, by recycling one million cell phones, a company can recover 50 pounds of gold, 550 pounds of silver, 20 pounds of palladium, and 20,000 pounds of copper—for a total value of $2.5 million.

Between 50 percent and 80 percent of the world's e-waste is shipped to sites in China, India, Pakistan, the Philippines, and Vietnam—places where recycling is often not managed in an environmentally sound manner. Emissions from these recycling sites damage human health and the environment. For example, residents of Guiyu—an agglomerate of four adjoined villages in Guangdong Province, China, that is widely perceived as the largest e-waste recycling site in the world—experience high rates of digestive, neurological, respiratory, and bone problems. In fact, some 80 percent of Guiyu's children experience respiratory ailments and are considered to be at high risk of lead poisoning. Above-average miscarriage rates are also reported in the region. Wind disperses particles released by open-air burning from this site across the Pearl River Delta Region, which has a population of 45 million people, enabling toxic chemicals from e-waste to enter the soil-crop-food pathway.

The Resource Conservation and Recovery Act (RCRA) gives the U.S. Environmental Protection Agency the authority to control hazardous waste, including the generation, transportation, treatment, storage, and disposal of such waste. The RCRA regulations are contained in title 40 of the Code of Federal Regulations (CFR) parts 239 through 282. However, due to various federal exemptions, it's legal to export almost all e-waste from the United States to developing countries provided a company obtain the country's consent to do so. The EPA even has a "prior informed consent" process for this purpose.

The United States is the only nation in the developed world that has not yet ratified the Basel Convention on hazardous waste. This is an international treaty designed to reduce the movement of hazardous waste between nations, and specifically to prevent transfer of hazardous waste from developed to less developed countries. Because the United States has signed but not yet ratified the Basel Convention, it is technically free to ship its e-waste abroad. However, some of the countries accepting much of the e-waste from the United States, such as China and Ghana, are actually forbidden from importing such trash because they have ratified the treaty.

Dell Inc. is a multinational computer technology company and is a subsidiary of Dell Technologies, a large technology company with some 138,000 employees. Dell manufactures, sells, repairs, and supports computer peripherals, data storage devices, network switches, personal computers, and servers.

Dell Reconnect is a partnership with Goodwill that began in 2004 with the goal of offering free and responsible computer recycling. Its participants can take their used computer equipment—of any brand and in any condition—and drop them off at one of more than 2,000 participating Goodwill locations. There the staff will examine each piece of equipment to determine whether to reuse, refurbish, or recycle it. Reuse means that the device is in good working order and can be resold after being cleaned and tested by technicians. Refurbish means that a device must be upgraded or repaired before resale. Equipment that cannot be reused or refurbished is broken down securely and recycled responsibly, through Dell, so that their valuable materials can be captured and put into new products.

Dell has collected more than 6.6 million tons of e-waste since 2007—through its Reconnect program as well as through its Asset Resale and Recycling Services program for business customers. Dell's partnership with Goodwill also funds the nonprofit's work, which is focused on job creation and skills training for people facing challenges in finding employment. In addition, the reused and refurbished equipment, which is sold through Goodwill stores, provides many families with the ability to buy computer products at an affordable price.

In 2009, Dell became the first in the IT industry to ban the export of nonworking electronics and e-waste to developing countries by its employees and business partners. Dell does not permit e-waste to be exported from developed countries (member countries in the Organisation for Economic Co-Operation and Development or the European Union) to developing (non-OECD/EU) countries, either directly or through intermediaries.

A two-year study by the Basel Action Network (BAN), a Seattle-based environmental watchdog organization, involved placing GPS tracking devices into 200 pieces of electronic equipment destined for recycling and then tracking their whereabouts. The researchers found that instead of being recycled in the United States, roughly one-third of these devices were exported overseas. Of the 28 electronics BAN dropped off with Dell Reconnect, six went abroad—to mainland China, Hong Kong, Taiwan, and Thailand. By some definitions, each of these countries could be classified as developing.

Both Goodwill and Dell have strong reputations for social and environmental responsibility. Their joint Dell Reconnect program is based on good intentions; however, it appears that tougher policies with greater due diligence and transparency are needed when it comes to e-waste management.

Critical Thinking Questions

1. What specific actions should Dell and Goodwill take to strengthen the Reconnect program? How can Dell monitor the large number of participants including employees and business partners at over 2,000 Goodwill locations to ensure that program functions as intended?
2. Why do you think it is that the United States, the largest generator of e-waste worldwide, is the only industrialized nation that has not yet ratified the Basal Convention?
3. Do research to learn of any proposed or pending legislation intended to close some of the gaps in current federal law. Write a brief summary of your findings.

Sources: "Basel Convention Overview," United Nations Environment Programme, www.basel.int/Implementation/Ewaste/Overview (accessed May 24, 2017); Lucy McAllister, "The Human and Environmental Effects of E-Waste," Population Reference Bureau, April 2013, www.prb.org/Publications/Articles/2013/e-waste.aspx; "Basic Information on the Resource Conservation and Recovery Act (RCRA) Export and Import Requirements," United States Environmental Protection Agency, https://www.epa.gov/hwgenerators/basic-information-resource-conservation-and-recovery-act-rcra-export-and-import (accessed May 28, 2017); Andrew Deck, "The Dell Reconnect Program Provides Solutions to E-waste," Dell, Inc., March 13, 2016, https://blog.dell.com/en-us/the-dell-reconnect-program-provides-solutions-to-e-waste/; Jessica Lyons Hardcastle, "Dell Investigating E-Waste Management Following Watchdog Group's Misconduct Claims," *Environmental Leader*, May 11, 2016, https://www.environmentalleader.com/2016/05/dell-investigating-its-e-waste-management-following-watchdog-groups-claims-of-misconduct/; "Current Member Spotlight: Electronic Recyclers International (ERI)," https://nerc.org/advisory-members/member-spotlight/2015/03/electronic-recycling-international-(eri) (accessed May 25, 2017); Ken Christensen and Katie Campbell, "The US Is Still Dumping Some of Its Toxic e-Waste Overseas," *PRI*, June 2, 2016, https://www.pri.org/stories/2016-06-02/us-still-dumping-some-its-toxic-e-waste-overseas; "Recycling Your Dell—Responsible Recycling: Dell Bans E-Waste Exports," Dell Inc., www.dell.com/learn/al/en/alcorp1/corp-comm/e-waste (accessed May 26, 2017); "Federal Legislation and Policy on E-Waste," Electronics TakeBack Coalition, www.electronicstakeback.com/promote-good-laws/federal-legislation/; Tom Risen, "America's Toxic Electronic Waste Trade," *U.S. News & World Report*, April 22, 2016, https://www.usnews.com/news/articles/2016-04-22/the-rising-cost-of-recycling-not-exporting-electronic-waste.

End Notes

[1] "Executive Order No. 11246, September 28, 1965, 30 F.R. 12319, Equal Employment Opportunity," https://www.eeoc.gov/eeoc/history/35th/thelaw/eo-11246.html.

[2] Bryce Covert, "Google Accused of 'Extreme' Discrimination Against Female Employees," *Think Progress*, April 10, 2017, https://thinkprogress.org/google-systemic-wage-gap-89c58f522dc8.

[3] Martyn Williams, "U.S. Alleges System Employment Discrimination at Oracle," *PC World*, January 18, 2017, www.pcworld.com/article/3159165/legal/us-alleges-systemic-employment-discrimination-at-oracle.html.

[4] Madeline Farber, "Qualcomm Is Paying Almost $20 Million After Claims It Didn't Pay Women Equally," *Fortune*, July 27, 2016, http://fortune.com/2016/07/27/qualcomm-settlement-equal-pay/.

[5] Sam Levin, "Google Accused of 'Extreme' Gender Pay Discrimination by US Labor Department," *The Guardian*, April 7, 2017, https://www.theguardian.com/technology/2017/apr/07/google-pay-disparities-women-labor-department-lawsuit.

[6] "US Department of Labor Settles Charges of Hiring Discrimination with Silicon Valley Company," U.S. Department of Labor, April 25, 2017, https://www.dol.gov/newsroom/releases/ofccp/ofccp20170425.

[7] Jon Swartz, "90 Age-Discrimination Complaints Reflect Growing Issue for Tech," *USA Today*, November 22, 2016, https://www.usatoday.com/story/tech/news/2016/11/22/90-age-discrimination-suits-reflect-growing-issue-tech/93110594/.

[8] "Contingent Workforce: Size, Characteristics, Earnings, and Benefits," U.S. Government Accountability Office, www.gao.gov/assets/670/669766.pdf.

[9] Elka Torpey and Andrew Hogan, "Working in a Gig Economy," *Career Outlook*, May 2016, https://www.bls.gov/careeroutlook/2016/article/what-is-the-gig-economy.htm.

[10] "Intuit 2020 Report: Twenty Trends That Will Shape the Next Decade," Intuit, October 2010, https://http-download.intuit.com/http.intuit/CMO/intuit/futureofsmallbusiness/intuit_2020_report.pdf.

[11] "Contingent Worker Sues Google Claiming IC Misclassification," *Staffing Industry Analysts*, November 14, 2014, www2.staffingindustry.com/Editorial/Daily-News/Contingent-worker-sues-Google-claiming-IC-misclassification-32231.

[12] "What Is H-1B Visa?," Path2USA, www.path2usa.com/what-is-h1b-visa (accessed June 17, 2013).

[13] "Characteristics of H-1B Specialty Occupation Workers," U.S. Department of Homeland Security, March 17, 2016, https://www.uscis.gov/sites/default/files/USCIS/Resources/Reports%20and%20Studies/H-1B/H-1B-FY15.pdf.

[14] Ibid.

[15] Haeyoun Park, "How Outsourcing Companies Are Gaming the Visa System," *New York Times*, November 10, 2015, https://www.nytimes.com/interactive/2015/11/06/us/outsourcing-companies-dominate-h1b-visas.html.

[16] Dawn Kawamoto, “8 Biggest H-1B Employers in 2015,” *InformationWeek*, March 24, 2016, www.informationweek.com/government/8-biggest-h-1b-employers-in-2015/d/d-id/1324807?image_number=9.

[17] “Computer and Information Technology Occupations,” Bureau of Labor Statistics, https://www.bls.gov/ooh/computer-and-information-technology/mobile/home.htm (accessed April 20, 2017).

[18] “Digest of Educational Statistics,” National Center for Educational Statistics, https://nces.ed.gov/programs/digest/d16/tables/dt16_322.10.asp?current=yes (accessed April 20, 2017).

[19] Hal Salzman, Daniel Kuehn, and B. Lindsay Lowell, “Guestworkers in the High-Skill U.S. Labor Market,” Economic Policy Institute, April 24, 2013, www.epi.org/publication/bp359-guestworkers-high-skill-labor-market-analysis/.

[20] John Bound, Gaurav Khanna, and Nicholas Morales, “Understanding the Economic Impact of the H-1B,” Population Studies Center, University of Michigan Institute for Social Research, Report 16-857, February 2017, www.psc.isr.umich.edu/pubs/pdf/rr16-857.pdf.

[21] Dr. Andrew Chamberlain, “Dispelling Myths: What H-1B Visa Workers Are Really Paid,” Glassdoor, April 3, 2017, https://www.glassdoor.com/research/h1b-workers/.

[22] “Stonewood Financial Is Answering Customer Retirement Questions Faster Thanks to GlowTouch,” GlowTouch Technologies, https://www.glowtouch.com/clients/stonewood-financial-retirement-income-solution/ (accessed May 11, 2017).

[23] “IBM Fires Workers, Offshores Jobs Despite Pledge to Trump,” *Bloomberg News*, January 23, 2017, www.investors.com/news/ibm-fires-workers-offshores-jobs-despite-pledges-to-trump/.

[24] Duncan Tucker, “More Than Twice as Many US Tech Firms Are Outsourcing IT Services from Abroad as in 2013,” *Near Shore Americas*, March 16, 2015, www.nearshoreamericas.com/tech-firms-outsourcing-services-2013/.

[25] Ritika Trikha, “Which Country Would Win in the Programming Olympics?,” Hacker Rank, August 25, 2016, https://blog.hackerrank.com/which-country-would-win-in-the-programming-olympics/.

[26] Matt Richtel, “Egypt Cuts Off Most Internet and Cell Service,” *New York Times*, January 28, 2011, www.nytimes.com/2011/01/29/technology/internet/29cutoff.html?_r=0.

[27] “FirstBest,” https://www.syntelinc.com/about-us/partners# (accessed May 11, 2017).

[28] “Outsourcing Risk: Who Pays Most When Customer Data Is Breached?,” Arizona State University, March 24, 2015, https://research.wpcarey.asu.edu/outsourcing-risk-who-pays-most-when-customer-data-is-breached/.

[29] Sarah McBride, “Oracle Whistleblower Suit Raises Questions Over Cloud Accounting,” *Reuters*, June 6, 2016, www.reuters.com/article/us-oracle-lawsuit-accounting-idUSKCN0YS0X1.

[30] Alexander J. Martin, “Oracle Settles Court Spat with Fired Cloud ‘Sales Inflation Whistle-blower,’” *The Register*, February 20, 2017, https://www.theregister.co.uk/2017/02/10/oracle_settles_court_case_with_fired_cloud_services_financials_whistleblower/.

[31] "Topic: False Claims Law," Fact Bites, www.factbites.com/topics/False-Claims-Law (accessed May 12, 2017).

[32] Ibid.

[33] Ibid.

[34] "Justice Department Recovers Over $4.7 Billion from False Claims Act Cases in Fiscal Year 2016," Department of Justice, December 14, 2016, https://www.justice.gov/opa/pr/justice-department-recovers-over-47-billion-false-claims-act-cases-fiscal-year-2016.

[35] See Note 31.

[36] Federal Accountability Initiative for Reform, "The Whistleblower's Ordeal," http://fairwhistleblower.ca/wbers/wb_ordeal.html (accessed June 18, 2013).

[37] Jaikumar Vijayan, "Scope of TJX Data Breach Doubles: 94 Million Cards Now Said to Be Affected," *Computerworld*, October 24, 2007, www.computerworld.com/s/article/9043944/Scope_of_TJX_data_breach_doubles_94M_cards_now_said_to_be_affected.

[38] Steve Ragan, "TJX Fires Whistleblower—Was It Justified Action or Something Else?," *Tech Herald*, May 26, 2008, www.thetechherald.com/articles/TJX-fires-whistleblower-was-it-justified-action-or-something-else-(Update)/24.

[39] Brad Wells, "What Truly Makes a Computer 'Green'?" *OnEarth* (blog), September 8, 2008, www.onearth.org/node/658.

[40] "Electronics Waste Management in the United States Through 2009," U.S. Environmental Protection Agency, May 2011, EPA 530-R-11-002 www.epa.gov/wastes/conserve/materials/ecycling/docs/fullbaselinereport2011.pdf.

[41] "About EPEAT," EPEAT, www.epeat.net/about-epeat/ (accessed May 13, 2017).

[42] EPEAT Recognizing Environmental Performance, www.ricoh-usa.com/about/epeat/ (accessed June 20, 2013).

[43] "EPEAT Purchasers," EPEAT, www.epeat.net/participants/purchasers/ (accessed May 13, 2017).

[44] Wendy Koch, "Is Apple's Recyclable iPad Really Green? Do You Care?" *USA Today,* February 1, 2010, http://content.usatoday.com/communities/greenhouse/post/2010/01/is-apples-recyclable-chemical-free-ipad-really-green-/1.

[45] "Lenovo Think Green Products—Materials," Lenovo, www.lenovo.com/social_responsibility/us/en/materials/ (accessed May 13, 2017).

APPENDIX A

A BRIEF INTRODUCTION TO MORALITY

By Clancy Martin, Assistant Professor of Philosophy, University of Missouri—Kansas City

INTRODUCTION

This appendix offers a quick survey of various attempts by Western civilization to make sense of the ethical question "What is the good?" As you will recall from Chapter 1, *ethics* is the discipline dealing with what is good and bad and with moral duty and obligation. How should we live our lives? How should we act? Which goals are worth pursuing and which are not? What do we owe to ourselves and to others? These are all ethical questions.

The answers to these questions are provided in what we call *moralities* or *moral codes*. The Judeo-Christian morality, for example, attempts to tell us how we should live our lives, the difference between right and wrong, how we ought to act toward others, and so on. If you ask a question like "Is it wrong to lie?," the Judeo-Christian morality has a ready answer: "Yes, it is wrong to lie; it is right to tell the truth." Speaking loosely, we could also say that, according to Judeo-Christian morality, it is *immoral* to lie and *moral* to tell the truth.

Moralities, or moral codes, differ by time and place. According to some people—eighth-century BC Greeks, for example—it is not always wrong to lie, and it is not always right to tell the truth. So we are confronted with the *ethical* problem of choosing between different *moralities*. Some moralities may be better than others. It may even be true—as many thinkers have argued—that only *one* system of morality is ultimately acceptable. Thinking about ethics means thinking about the strengths and weaknesses of moralities, understanding why we might endorse one morality and reject another, and searching for better systems of morality or even "the best" morality. Especially in our own day, when globalization and accelerating advances in communication have created a cultural blending (and cultural conflicts) like never before, our ability to understand different moralities is crucial.

This appendix introduces you to the way various Western philosophers have answered the ethical question "What is the good?" Because the Western tradition is complicated enough, we have not addressed Eastern moralities and the ethical thinking of many fascinating Eastern philosophers. One of the interesting things about studying ethics is the enormous variety of moralities that humans have created and the many similarities between competing moralities. Unlike the rest of this textbook, this appendix is not specifically focused on the ethical problems created by technology. But as you read through the various moralities in the appendix, ask yourself how you would deal with the moral dilemmas you have studied and confronted in your own life.

THE KNOTTY QUESTION OF GOODNESS

Achilles kills Hector outside the gates of Troy. He binds Hector's corpse by the ankles, ties the ankles to the back of his chariot, and drags the body around the city walls. The treatment of the fallen Trojan hero by his victorious Greek enemy is so outrageous that not only Trojans, but most of Achilles' Greek allies and even the Gods, are shocked. But what is wrong with Achilles' action?

To an ancient Greek of the time, the answer would not have been obvious. When the poet **Homer (eighth century BC)** tells this story in his epic *The Iliad*, his purpose is to illustrate a failure in the morality of his own day. Among Greeks of Homer's day, the prevailing moral code was: "Help to friends and harm to enemies." That code may sound naïve or ridiculously simplistic today. But for the collection of small and largely independent city-states that was ancient Greece, it was a moral code that had worked reasonably well for centuries. Yet Homer saw that different times were on the way. When the Greeks banded together, as they did to combat the Trojans, the old morality looked barbaric. There was nothing heroic about the lone Achilles dragging his vanquished enemy behind him. On the contrary, he seemed like a savage.

When a society is passing from an old moral code to a new one, or when two different cultures clash in their moral codes, the extraordinarily difficult question of which moral code is correct inevitably appears. *Ethics*, the systematic study of moral codes, is the attempt to answer that question. Almost every philosopher and most thinking people will agree that some moral codes are better than others; many philosophers and others will argue that a particular moral code is the best.

Perhaps the most famous philosopher of all time, **Socrates (470–399 BC)**, argued that there was only one true moral code, and it was simple: "No person should ever willingly do evil." Socrates thought that no harm could come to a person who always sought the good, because what truly counted in life was the caretaking of one's self or soul. But Socrates also acknowledged that identifying the good was rarely easy, and his method of constantly interrogating his friends and fellow citizens—what came to be called Socratic questioning, or the Socratic dialectic—tried to improve everyone's thinking about what one ought and ought not do.

Socrates never wrote down any of his philosophy. But his student **Plato (427–347 BC)** made Socrates the hero of almost all of his many philosophical dialogues. Plato was the first "professional" philosopher in the West: he established a school of philosophy called the Academy (where we get the word *academic*), published a great number of books both for general readers and his own students, and formed arguments on virtually every subject in philosophy (not only morality). In fact, Plato possessed such breadth that the twentieth-century philosopher Lord Alfred North Whitehead wrote that "all subsequent philosophy is only a footnote to Plato."

In many of his dialogues Plato raises the question: “What is the good?” Like Homer (who was one of Plato’s favorite writers), Plato lived in a time when great political, social, and cultural changes were occurring. Athens had lost the first major war in its history, trade was accelerating across the Mediterranean, and people were traveling deeper into Asia and Africa and discovering new cultures, religions, and values. Many candidates for “the good” were being offered by different thinkers: some thought that “pleasure” was the highest good, others argued that “peace” (both personal and social) and what contributed to it was the best, others argued for “flourishing” and material wealth and power, while still others endorsed “honor and fame.” But Plato responded that, while all of these things might be examples of goodness, they were not good itself. What is it that makes them good? What is the nature of the property “goodness” that they all share? And because we recognize that most “goods” may also mislead us into badness—the good of pleasure is an obvious example—how shall we sort the good from the bad?

Plato’s idea is that we cannot reliably say what is good and what is not until we know what goodness is. Once we have identified goodness itself, we can discriminate among particular goods and particular activities that are designed to seek the good. We will judge what is “good” and “better” by comparing it with what is “best”: the truly and wholly good. And the truly and wholly good ought always and everywhere to be good. Could we say that something was truly, wholly good if it was good only in some countries and not others, during some times and not others? So, if we can identify goodness as such, Plato said, we can solve every problem posed by the clash between good and bad; that is, we can solve every problem of morality.

One way to think about Plato’s insight is to see the moral importance of *standards*. We have standards for good hamburgers, for good businesses, and for good hammers, so why not have standards for good people and good actions? A *standard* is one way of providing a *justification* for an evaluation. Suppose Rebecca insists, “It is always wrong to kill an innocent human being.” And Thomas replies, “But why?” Rebecca may justify her evaluation by appealing to a standard of rightness and wrongness. Of course, identifying that standard may prove more difficult than appealing to it, and the history of ethics, again, may be seen as the struggle to provide such a standard. The philosophers you will read about in the following sections attempted to answer Plato’s knotty questions in their own ways.

RELATIVISM: WHY “COMMON SENSE” WON’T WORK

What about simply using common sense to find the good? Some twentieth-century philosophers argued for what they called moral “intuitions”: a kind of “consult your conscience” approach to morality. This view is initially compelling for most people; it holds that the standard for goodness demanded by Plato is accessible to all of us if we simply think through our moral decisions carefully enough. (Socrates may have been arguing for the same view.) There is a “voice” in our heads that tells us what is morally right and wrong, and if you honestly and thoroughly interrogate yourself about what you ought to do, that “voice” will praise the right action and warn you against the wrong one. Someone who says “Do the right thing!” is invoking this commonsense notion. We all know what the right thing is, a moral intuitionist argues, if we use our common sense and are tough on ourselves. The difficulty is that we don't always want to use common sense or ask ourselves tough questions. Therefore, the problem of right and wrong is not so much that of moral knowledge as it is weakness of will. We *know* what we ought to do, but it is hard to make ourselves *do* it.

A crippling difficulty with this view is called the problem of relativism. *Cultural relativism* is the simple observation that different cultures employ different norms (or standards). Implicit in this view is that it is morally legitimate for different cultures to create and embrace different norms. So, for example, among the Greeks of Homer's day, lying was considered to be a virtue. Odysseus was praised specifically for his ability to lie well. In eighteenth-century Germany, on the other hand, lying was widely considered as morally reprehensible as theft. Some philosophers even argued that lying was just as morally foul as murder. For the relativist, lying is neither right nor wrong; rather, it can be right at a certain time and place and wrong in another. Another example is bribery. Although people in many nations condemn bribery, it is perfectly acceptable in other countries, particularly in Latin America. The relativist would say: "Bribery itself is not right or wrong. Rather, some people at some times and in some places say it is wrong, and other people say it is right, depending on the circumstances. Bribery is therefore wrong for some people, right for others."

You have probably encountered this relativism with something as simple as email. The conventions that govern email etiquette vary dramatically from user to user, group to group, and culture to culture. The emoticon-laced email you send to a friend would be wholly inappropriate if sent to a professor. The kind of language you use in an email to a college admissions officer is not what you would use to email your parents or an email pal in India. A practical platitude that embodies this idea is: "When in Rome, do as Romans." What is *appropriate* and what counts as a "good" email (as opposed to a "bad" or offensive email) depends on the conventions within its cultural context. Even emails have *norms*.

Moral relativists argue that all norms and values are relative to the cultures in which they are created and expressed. For the moral relativist, it makes no sense to say that there are any transcultural or transhistorical values, and that any attempt to construct them would still be informed by the particular cultural values of a person or group. All you can talk about are the values "on the ground": the values that particular cultures embrace. And common sense may be one of the best tools for discovering those values. Common sense may be the psychological embodiment of the complex structure of rules, standards, and values that are the substance of every robust culture.

But moral relativists run into trouble, because there are some moral claims they cannot consistently make. Moral relativists can say "slavery is wrong in my society" or "slavery is wrong in the twentieth century," but they cannot say that slavery is always wrong. Furthermore, because they cannot appeal to transcultural standards for morality, they cannot speak of *moral progress*. Moral values (like all other values) change over time for the relativist, but they do not improve or degenerate. Yet, most of us would agree that the growing worldwide prohibition against slavery and torture, for example, is not merely a change, it is moral progress. And if we believe in moral progress, we cannot be relativists.

Egoism versus Altruism

Throughout this book we have seen that ethics deals with the question of how we should treat one another. But some thinkers would say we have already misconstrued the question when we ask "How should we treat others?" For an *egoist*, the salient moral question is "How do I best benefit myself?," and the answer to Plato's question "What is the good?" is simply "The good is whatever is pleasing to *me*."

Egoism is usually divided into two types. *Psychological egoism* is the thesis that people always act from selfish motives, whether they should or not. *Ethical egoism* is the more controversial thesis that, whether people always act from selfish motives, they should if they want to be moral.

There is a superficial plausibility to psychological egoism, because it might appear that most of us make many of our choices for self-interested reasons. You probably decided that you wanted to go to college rather than immediately finding a job. You might respond: "No, I went to college because my parents wanted me to!" But the psychological egoist would reply: "That simply means that, for you, pleasing your parents is more important than other things that would have kept you out of college."

However, some of the problems with psychological egoism already are glaringly apparent. First, though we may make many decisions based on our own interests, it is far from obvious that *all* of our decisions are motivated by self-interest. We make many decisions, including decidedly uncomfortable ones, because we are thinking of the interests of others. It is silly to suppose that our own interests must always and implicitly conflict with those of others, as a psychological egoist believes. Why did you go to college? Because you wanted to, and your parents, teachers, and friends wanted you to. Everyone's interests happily coincided, and it is oversimplifying your complex choice to say, as a psychological egoist would, "I did it because *I* wanted to."

While considering ethical egoism, we should also look at its opposite: *altruism*. The altruist argues that the morally correct action always best serves the interest of others. Wouldn't the world be a better place, the altruist asks, if we worried about ourselves less and tried to help other people?

No one will deny that everyone benefits from altruism, but problems arise if we try to adopt altruism as a moral code. Practically speaking, it is sometimes difficult to know what best serves the interest of another, beyond helping people with the basic necessities of life. For example, a devout Southern Baptist might sincerely believe that his neighbors are condemned to hell unless they accept his religious views, and might feel an altruistic urge to convert them, despite their hesitation. Another more famous example involves a boat full of altruists lost at sea. They can only survive if one of them volunteers to be eaten, but if the only moral action is to serve the interests of others, how can any of the adrift altruists be truly moral when one of them has to die to save the rest?

Problems like these help to motivate advocates of ethical egoism. We do not reliably know the interests of others, the ethical egoist says, but we certainly know our own. And, unlike altruists, whose satisfaction is in helping others, ethical egoists try to create a happy and moral world by seeking good for themselves. The hacker who thinks she can morally break the rules because she has the smarts to do so is both a psychological egoist ("you would break the rules too, if you could") and an ethical egoist ("everyone who can break the rules to help themselves should do so"). Given the choice between self-interest and altruism, the ethical egoist takes the former.

Of course, the only choice is not between ethical egoism and altruism. Most moral codes and most people recognize the importance of both self-interest and the interest of others. The more telling objection to ethical egoism is that it does not respect our deepest intuitions about moral goodness. If an ethical egoist can serve his own interest by performing some horrific act against another human being, and be guaranteed that the act will not interfere with his self-interest, he is morally permitted to perform that act. In fact, if he finds that he can *only* serve his interest by performing the horrific act and getting away with it, he is morally *required* to do so. An employer who could benefit from spying on her employee's email would be morally required to do it if it served her long-term interest. But for most of us, such examples are sufficient to defeat ethical egoism. Moral codes are plausible only if they accommodate basic intuitions about our sense of right and wrong, and ethical egoism fails on that ground.

DEONTOLOGY, OR THE ETHICS OF LOGICAL CONSISTENCY AND DUTY

Most people find they cannot accept relativism as a moral code because of their moral intuitions that some things are *always* wrong (like slavery or the torture of innocents). For this reason, they must also abandon a "common sense" approach to morality, which relies on embedded knowledge of cultural norms. The problems with egoism and altruism are even more glaring. But don't despair—there are lots more moral theories to consider. The rest of this appendix reviews several modern attempts to articulate a consistent morality.

Immanuel Kant (1724–1804) is generally considered the most important philosopher since Aristotle. Kant's moral theory is an attempt to refine and provide a sound philosophical foundation for the strict Judeo-Christian morality of his own day. Most people, when they begin thinking about ethics in a philosophical way, find that they are some brand of Kantian. Kant's theory is called *deontology*, from the Greek word *deon*, meaning *duty*. For Kant, to do what is morally right is to do one's duty.

Understanding what one's duty requires is the difficult part, of course. Kant begins with the idea that the only thing in the world that is wholly good, without any qualification, is good will. Most good things may be turned to evil or undesirable ends, or are mixed with bad qualities. Human beings do not seem wholly good: they are a mix of good and bad. Money is a good that most of us seek, while "love of money is the root of all evil." But the will to do good—the desire or intention—must be wholly good. If we think through what we mean by "moral goodness," Kant argues, we realize that the notion of moral goodness is just another name for this will to goodness. Kant recognizes that, as the old saying goes, "the road to Hell is paved with good intentions"; he is not saying that good will must always have good consequences. (In general, Kant is suspicious of the moral worth of consequences.) But the intention to do good, before it gets tangled up in the difficulties of the world, must itself be purely good.

Morality, therefore, comes from our ability to intend that certain things happen: that is, from our ability to choose. The good choice will come from a good will. But how do we sort the good choice from the bad? Kant, following the ancient Greek philosopher Aristotle, believed that the property that makes human beings unique, and that propels us into the moral sphere, is the faculty of *reason*. Kant saw human beings as constantly torn between their passions, drives, and desires (what he called "inclinations") and the rational ability to make good choices on the basis of good and defensible reasons. For Kant, with his dim view of human nature, what we *want* to do is very rarely what we *ought* to do. But we can recognize what we ought to do by the application of reason.

Kant's derivation of the *categorical imperative*, which he argued is the fundamental principle of all morality, is notoriously complex. But the key idea is simple: reason demands consistency and rejects contradiction. Accordingly, Kant argued that the moral principle we should follow must preserve consistency in all cases and prevent any possibility of contradiction. This moral principle might be expressed as: "Act only on that maxim such that the maxim of your action can be willed to be a universal law." (Although Kant offered several different formulations of the categorical imperative, this is the most famous and most basic formulation.) Kant's prose is dense and confusing, and the categorical imperative is no exception. What does Kant mean?

Kant observed that we make choices according to rules. We tell the truth even when it is inconvenient or embarrassing because we have a rule in our heads that tells us to do so. This is an example of what Kant calls a "subjective principle of action" or a *maxim*. Other examples of maxims are "don't steal" and "keep your promises." Our heads are full of rules that we use to guide our choices. When we worry about *moral* choices, Kant tells us in the categorical imperative that we should act only on choices that "can be willed to be a universal law." That is, before acting on a maxim that informs a moral choice, one must ask: "Could this rule (this maxim) be applied to everyone, everywhere, for all time?" Kant argues that, by *universalizing* a maxim, one can see whether it generates a contradiction. If it generates a contradiction, it cannot be rational, and so it is not a legitimate expression of a good will. If it does not generate a contradiction, it looks morally permissible. When we follow the categorical imperative, Kant thinks, we are doing our (moral) duty.

Take a couple of examples. Suppose you decide to borrow money without intending to pay it back. Your maxim might be: "If I need to borrow money I should do so, even though I know I will never pay it back." Now universalize this maxim according to the categorical imperative. Suppose everyone, everywhere, always borrowed money without the intention of paying it back? Obviously no one would lend money and the very possibility of borrowing would be eliminated. It is rationally contradictory to choose borrowing money without intending to pay it back.

Or, suppose you are caught cheating and try to lie your way out of it. Your maxim is: "When caught cheating, I should lie to get out of trouble." But suppose everyone, everywhere, always lied to get out of trouble when caught cheating? To lie you must hide the truth, and in this situation, were it universalized, it would be impossible to hide the truth. Lies depend on being exceptions to the rule of truthful communication; if lies are no longer the exception but the rule, there is no more truthful communication, and a lie becomes impossible. Again, this is a rational contradiction, and we see that the lie is immoral.

Suppose, however, that you try a maxim like "Thou shalt not kill." What if everyone, everywhere, always avoided killing others? No contradiction is generated. There may be many impractical consequences of universal not-killing, but there are no logical problems with it. If you try a maxim of "Thou shalt kill," on the other hand, you see how quickly it falls apart.

It is not difficult to generate objections to this theory. If one makes maxims specific enough, it is easy to justify apparently immoral actions while following the rule of universal maxims. For example, one can easily universalize a maxim like "a woman with no money whose children are dying of pneumonia should steal penicillin if necessary to save her children's lives," yet Kant would maintain that theft is always wrong and irrational.

Kant also maintains that it is always irrational and wrong to lie, even in the attempt to save an innocent life. But to most of us that sounds absurd. Should a mother never lie, even if it means saving the life of her child? Should the Danes who lied to the Nazis about whether they were protecting Jews have told the truth? Surely not.

Perhaps the most controversial aspect of Kant's moral theory is his distinction between moral duty and happiness. Kant argues that choosing freely on the basis of what we rationally see is right—following the categorical imperative, acting from duty—is the only way we can choose *morally*. But suppose we are acting a certain way solely because it makes us happy, even though those actions happen to agree with what would otherwise be our duty. For Kant, actions motivated by inclination (with the result of happiness) are not motivated by duty, and so we should not consider them *moral* actions. For example, a suicidal person who does not shoot herself because she recognizes that it would be irrational (and thus contrary to her duty) is acting morally. However, another person who fleetingly considers shooting himself but then declines because he loves his life is not acting morally; he is merely inclining toward his happiness.

But if moral duty and happiness are opposed, it seems that only miserable people can be moral. Wouldn't it be nicer if we could have both moral worth in our actions and happy lives? This leads us to *utilitarianism*, the theory of morality that responds specifically to deontology by insisting that morality and happiness are not opposites, but the very same thing.

HAPPY CONSEQUENCES, OR UTILITARIANISM

Hedonism is the notion, first advocated by the Greek philosopher Epicurus (342–270 BC), that pleasure is the greatest good for human beings. (Epicurus is the source of the word *epicurean*.) To be moral is to live the life that produces the most pleasure and avoids pain. But we should not suppose that Epicurus was arguing for a life of debauchery. Drinking too much wine, for example, though fun while it lasts, produces more pain than pleasure in the end, so Epicurus sorted pleasures into categories:

- Natural and necessary, like sleeping and moderate eating
- Natural but unnecessary, like drinking wine or playing chess
- Unnatural and unnecessary, which hurt one's body (e.g., smoking cigarettes)
- Unnatural but necessary (but there are no such pleasures)

Epicurus said that we should cultivate natural and necessary pleasures, enjoy natural but unnecessary pleasures in moderation, and avoid all other sorts. The true hedonist does not seek what is immediately pleasurable, but looks for pleasures that will guarantee a long, healthy life full of them. For this reason, *friendship* is Epicurus' favorite example of a pleasure that everyone should cultivate; friendship was consistently considered one of the highest human goods among ancient Greeks.

Jeremy Bentham (1748–1832) adopted Epicurus' basic principles when he developed the theory that later became known as *utilitarianism*. In response to Plato's question "What is the good?," Bentham argued that it is easy to see what humans consider good because they are always seeking it: pleasure. But Bentham was not an egoist, and he argued that the highest good would result from a maximum of pleasure for all people concerned in any moral decision. Decisions that promote *utility* are those that create the most pleasure (the words *utility* and *pleasure* were virtually interchangeable to Bentham, though later utilitarians would ascribe many different meanings to *utility*). Whenever making a decision, the person who desires a moral result should weigh all possible outcomes, and choose the action that produces the most pleasure for everyone concerned. Bentham called this weighing of outcomes a "utilitarian calculus."

Bentham's new moral theory enjoyed enormous popularity, but brought inevitable objections. Some philosophers argued that such a theory made people look no better than swine (because they were just pursuing pleasure). Others objected that people would surely frame their moral decisions to enable them to do whatever they pleased. **John Stuart Mill (1806–1873)** responded to these objections and gave us the form of utilitarianism that, in its fundamentals, is the same moral theory that so many philosophers and economists still endorse today.

Mill argued that the good that human beings seek is not so much pleasure as happiness, and that the basic principle of utilitarianism was what he called the "Greatest Happiness Principle": that action is good which creates the greatest happiness, and the least unhappiness, for the greatest number. He also insisted that people who used this principle must adopt a disinterested view when deciding what would create the greatest happiness. He called this the perspective of "the perfectly disinterested benevolent spectator."

When making a moral decision, then, people will consider the various outcomes and make the choice that produces the most happiness for themselves and everyone else. This is not the same as asking which choice will produce the most pleasure. Accepting a job selling computer software for $55,000 a year might produce more short-term pleasure than going to graduate school, but it might not produce the most happiness. You might be broke and hungry in graduate school, but still very happy because you are progressing toward a goal and finding intellectual stimulation along the way.

The utilitarian must also ask: does this decision produce the most happiness for everyone else, and am I evaluating their happiness fairly and reasonably? Suppose that the recent graduate is again deliberating whether to go to graduate school. Her mother and her father, both attorneys, very much want her to go into the law. But she is fed up with school and will be miserable sitting in a classroom all day. She is sick of eating Ramen noodles and having roommates, and would like to drink a nice bottle of wine once in a while and buy a new car. It is true that her parents' happiness is relevant to the decision, but she must try to weigh the happiness of everyone involved. How unhappy will her parents be if she takes a few years off? How unhappy will she be back in a lecture hall? Utilitarians admit that finding the good is not always easy, but they insist that they offer a practical method for finding the good that anyone can use to solve a moral dilemma.

Utilitarianism is a kind of *consequentialism*, because we evaluate the morality of actions on the basis of their probable outcomes or consequences. For this reason utilitarianism is also what we call a *teleological* theory. Coming from the Greek word *telos*, meaning *purpose* or *end*, teleology refers to the notion that some things and processes are best understood by considering their goals. For utilitarians the goal of life is happiness, and thus they argue that the good (moral) life for humans is the happy life.

Utilitarianism is probably the most popular moral theory of the last hundred years. It is widely used by economists, because one easy way of measuring utility is by assigning dollar signs to outcomes. Today's most famous advocate of animal rights, Peter Singer, is also a well-known utilitarian. Many different versions of utilitarianism have been advanced. In *rule-utilitarianism*, we first rationally determine the general rules that will produce good outcomes, and then follow those rules. In *preference-utilitarianism*, we solve the difficult problem of what will create the most happiness for others by simply asking every person involved for their preference.

But there are many strong objections to utilitarianism. One was raised by the German philosopher **Friedrich Nietzsche (1844–1900)** in his masterpiece *Thus Spoke Zarathustra*. At the end of the book, Zarathustra asks himself if his efforts to find the good for human beings and for himself have increased his personal happiness. He responds to himself: "Happiness? Why should I strive for happiness? I strive for my work!" Nietzsche's point is that many profound and praiseworthy human goals are unquestionably moral, and yet they cannot be said to contribute to the happiness of the person who has those goals, and perhaps not even to the happiness of the greater number. It is true that Van Gogh's paintings, though they destroyed him, created a greater happiness for the rest of us. But that did not count for him as a reason to paint them—he had no idea of his own legacy. For a utilitarian, such self-sacrifice is not only confused but immoral. And yet if our moral theory has difficulty accounting for the value of Van Gogh sacrificing his happiness and everything he loved to his art, we might be in trouble.

Perhaps the most telling objection to utilitarianism is that it could be used to morally sanction a "tyranny of the majority." Suppose you could solve all of the suffering of the world and create universal happiness by flipping a switch on a black box. But, in order to power the box, you had to place one person inside it, who would suffer unspeakably painful torture. None of us would be willing to flip that switch, and yet for a utilitarian such an action would not only be permissible, it would be morally demanded.

A related objection comes from the British philosopher Bernard Williams. Suppose you are an explorer in the Amazon basin and you stumble on a tribe that is about to slaughter 20 captured warriors from another tribe. You interrupt the gruesome execution, and the tribal chief offers to release 19 prisoners in your honor, on the condition that you accept the ceremonial role of choosing one victim and killing him yourself. A utilitarian would be morally required to accept, but most of us would be morally appalled at the idea of killing a complete stranger who presented no threat to us.

Utilitarians have responded to such objections by introducing the notion of certain irreducible human *rights* into utilitarianism. The discussion now turns to these rights and their origins in *social contract theory*.

Promises and Contracts

Although there are good reasons for being suspicious of egoism of any stamp, **Thomas Hobbes (1588–1679)** was a psychological egoist, which was essential to his moral and political theory. Hobbes argued that there are two fundamental facts about human beings: (1) we are all selfish and (2) we can only survive by banding together. You may have heard Hobbes' famous dictum that human life outside of a society—that is, in his imagined "state of nature"—is "solitary, poor, nasty, brutish, and short." We form groups for self-interested reasons because we need one another to survive and prosper. But the fact that we band together as selfish beings inevitably results in tension between people. Because resources are always scarce, there is competition, and competition creates conflict. Accordingly, if we are to survive as a group, we need rules that everyone promises to follow. These rules, which may be simple at first but become enormously complex, are an exchange of protections for freedoms. "I promise not to punch you in the nose as long as you promise not to punch me in the nose" is precisely such an exchange. You trade the freedom to throw your fists wherever you please for the protection of not being punched yourself. These rules of mutual agreement are, of course, called *laws*, and they guarantee our protections or *rights*. The system of laws and rights that make up the society is called the *social contract*.

Social contract theory builds on the Greek notion that good people are most likely encouraged by a good society. Few social contract theorists would argue that morality can be reduced to societal laws. But most would insist that it is extremely difficult to be a good person unless you are in a good society with good laws. Hobbes argued that the habit of exchanging liberties for protections would extend itself into all dimensions of a good citizen's behavior. The law is an expression of the reciprocity expressed in the Golden Rule—"do unto others as you would have them do unto you"—and so through repeated obedience to the law we would develop the habit, Hobbes thought, of treating others as we would like to be treated.

The most famous American social contract theorist was **John Rawls (1921–2002)**. Rawls argued that "justice is fairness," and for him the morally praiseworthy society distributes its goods in a way that helps the least advantaged of its members. Rawls asked us to imagine what rules we would propose for a society if, when we thought about the rules, we imagined that we had no idea what our own role in that society would be. What rules would we want for our society if we did not know whether we would be poor or rich, African American or Native Indian, man or woman, or a teacher, plumber, or famous actor? Rawls imagined that this thought experiment—which he called standing behind "the veil of ignorance"—would guarantee fairness in the formulation of the social contract. Existing social rules and laws that did not pass this test—that no rational person would endorse if standing behind the veil of ignorance—were obviously unfair and should be changed or discarded.

Strictly speaking, social contract theory is not a moral code. But because so many of our moral decisions are made in the context of laws and rights, we should understand that the foundation of those laws and rights is a system of promises that have been made, either implicitly or explicitly, by every citizen who freely chooses to live in and benefit from a commonwealth.

A RETURN TO THE GREEKS: THE GOOD LIFE OF VIRTUE

In the twentieth century, many philosophers grew increasingly suspicious of the possibility of founding a workable moral system upon rules or principles. The problem with moral rules or principles is that they self-consciously ignore the particulars of the situations in which people actually make moral decisions. For the dominant moralities of the twentieth century, deontology and utilitarianism, what is moral for one person is moral for another, regardless of the many differences that undoubtedly exist between their lives, personalities, and stations. This serious weakness in prevailing moral systems caused philosophers to turn once more to the ancient Greeks for help.

Aristotle (384–307 BC) argued that it does not make sense to speak of good actions unless one recognizes that good actions are performed by good people. But good people deliberate over their actions in particular situations, each of which may differ importantly from other situations in which a person has to make a moral choice. But what is a good person?

Aristotle would have responded to this question with his famous "function argument," which posits that the goodness of anything is expressed in its proper function. A good hammer is good because it pounds nails well. A good ship is good if it sails securely across the sea. A bad ship, on the other hand, will take on water and drift aimlessly across the waves. Moreover, we can recognize the function of a thing by identifying what makes it different from other things. The difference between a door and a curtain lies fundamentally in the way they do their jobs. Human function, the particular ability that makes mankind different from all other species, is the ability to reason. The good life is the life of the mind: to be a good person is to actively think.

But to pursue the life of the mind, we need many things. We need health; we need the protection and services of a good society; we need friends for conversation. We need leisure time and enough money to satisfy our physical needs (but not so much as to distract or worry us); we need education, books, art, music, culture, and pleasant distractions to relax the mind.

This does sound like the good *life*. But how does the thinking person *act*? Presumably, Aristotle's happy citizen will encounter moral conflicts and dilemmas like the rest of us. How do we resolve these dilemmas? What guides our choices?

Aristotle did not believe that human beings confront each choice as though it were the first they ever made. Rather, he thought, we develop habits that guide our choices. There are good habits and bad habits. Good habits contribute to our flourishing and are called *virtues* (Aristotle's word, *arête*, may also be translated as *excellence*). Bad habits diminish our happiness and are called *vices*. And happily, for Aristotle, the thinking person will see that there is a practical method for sorting between virtues and vices built into the nature of human beings. Aristotle insisted that human beings are animals, like any other warm-blooded creature on the earth; just as a tiger can act in ways that cause it to flourish or fail, so human beings have a natural guide to their betterment. This has come to be called Aristotle's "golden mean": the notion that our good lies between the extremes of the deficiency of an activity and its excess. Healthy virtue lies in moderation.

An example will help. Suppose you are sitting in the classroom with your professor and fellow students when a wild buffalo storms into the room. The buffalo is enraged and ready to gore all comers. What do you do? An excessive action would be to attack the buffalo with your bare hands: this would, for Aristotle, show the vice of rashness. A deficient action would be to cower behind your desk and shriek for help: this would show the vice of cowardice. But a moderate action would be to make a loud noise to frighten the buffalo, or perhaps to distract it so that others could make for the door, or to do whatever might reasonably reduce the danger to others and yourself. This moderate course of action exemplifies the virtue of courage. Notice, however, that the courageous course of action would change if an enraged tomcat came spitting into the room. Then the moderate and virtuous choice might be to trap the feline with a handy trash basket.

Aristotle's list of virtues includes courage, temperance, justice, liberality or generosity, magnificence (living well), pride, high-mindedness, aspiration, gentleness, truthfulness, friendliness, modesty, righteous indignation, and wittiness. But one could write many such lists, depending on one's own society and way of life. Aristotle would doubtless argue that at least some of these virtues are virtuous for any human being in any place or time, but a strength of his theory is that others' virtues depend on the when, where, and how of differing human practices and communities. One appeal of virtue ethics is that it insists on the context of our moral deliberations.

But is human goodness fully expressed by moderation? Or by being a good citizen? And what about people who lack Aristotle's material requirements of health, friends, and a little property? Aristotle is committed to the idea that such people cannot live fully moral lives, but can that be right? As powerful as it is, one weakness of Aristotle's virtue ethics is that it seems to overemphasize the importance of "fitting" into one's society. The rebel, the outcast, or the romantic chasing an iconoclastic ideal has no place. And Aristotle's theory may sanction some gross moral injustices—such as slavery—if they contribute to the flourishing of society as a whole. Aristotle himself would have had no problem with this: his theory was explicitly designed for the aristocratic way of life. But today we would insist that the good life, if it is to be truly *good* for any of us, must at least in principle be available to every member of our society.

Feminism and the Ethics of Care

Psychologist and philosopher **Carol Gilligan** discovered that moral concepts develop differently in young children. Boys tend to emphasize reasons, rules, and justifications; girls tend to emphasize relationships, the good of the group, and mutual nurturing. From these empirical studies Gilligan developed what came to be called the "ethics of care": the idea that morality might be better grounded on the kind of mutual nurturing and love that takes place in close friendships and family groups. The ethical ideal, according to Gilligan, is a good mother.

Gilligan's ethics of care is compelling because it seems to reflect how many of us make our daily moral decisions. Consider the moral decisions you face in a typical day: telling the truth or lying to a parent or sibling, skipping a party to take care of a heartsick friend or going to see that cute guy, keeping a promise to another student to copy your notes or saying "oops, I forgot." We often confront the moral difficulties of being a good son, sister, friend, or colleague. Generally speaking, we do not settle these moral issues on the basis of impersonal moral principles—we wonder whether it would even be appropriate to do so, given that we are personally involved in these decisions. Should you treat your best friend in precisely the same way you treat a stranger on the street? Some moralists would say, "Of course!" Yet, many of us would consider such behavior odd or psychologically impossible.

The feminist attack on traditional ethics does not accuse one Western morality or another, but indicts its whole history. Western morality has insisted on rationality at the expense of emotions, on impartiality at the expense of relationships, on punishment at the expense of forgiveness, and on "universal principles" at the expense of real, concrete moral problems. In a phrase, morality has been male at the expense of the female. Thus, the feminist argues, a radical rethinking of the entire history of morality is necessary.

As a negative attack on traditional morality, it is hard to disagree with feminism. Our moral tradition does have a suspiciously masculine cast; it is not surprising that virtually every philosopher mentioned in this appendix was a man. But feminism has struggled to develop a positive ethics of its own. Many consider Gilligan's ethics of care to be the best attempt so far, and it works well in family contexts. But when we try to extend the ethics of care into larger spheres, we run into trouble. Gilligan insists on the moral urgency of partiality (as a mother is partial to her children, and even among children). But you would object if you were a defendant in a lawsuit and saw the plaintiff enter, wave genially to the judge, and say, "Hi Mom!" The point, of course, is that in many situations we insist on *impartiality*, and for good reasons. And we all agree that people we have never met may still exercise moral demands upon us. We believe that a man rotting in prison on the other side of the world ought not be tortured, and maybe that we should do something about it if he is (if only by donating money to Amnesty International). Everyone deserves protection from torture for reasons that apply equally to all of us.

PLURALISM

When the German philosopher Nietzsche famously proclaimed that "God is dead," he was not proposing that the nature of the universe had changed. Rather, he was proposing that a change had taken place in the way we view ourselves in the universe. He meant that the Judeo-Christian tradition that has informed all of our values in the West can no longer do the job for us that it used to do. Part of that tradition, Nietzsche thought, was the unfortunate Platonic idea that there is an answer to the question "What is the good?" There is no more one "good" than there is one "God" or one "truth": there are, Nietzsche insisted, many goods, like there are many truths. Nietzsche argued the moral position that we now call *pluralism*.

Pluralism is the idea that there are many goods and many sources of value. Pluralism is explicitly opposed to Plato's insistence that all good things and actions must share some quality that makes them all good. But does this make the pluralist a relativist? No, because the pluralist argues for the moral significance of two ideas that the relativist rejects: (1) that some aspects of human nature are transcultural and transhistorical and (2) that some methods of inquiry reveal transcultural and transhistorical human values.

When we look at human history, we see goods that repeatedly contribute to human flourishing and evils that interfere with it. War is almost always viewed as an evil in history that has consistently interfered with human flourishing; health, on the other hand, is almost always viewed as a good (with the exception of aberrant religious practices like asceticism). "Avoid war and seek health" is not a moral code—although it might go further than we think—but it does provide an example of what a pluralist is looking for. The pluralist wants concrete goods and practices that actually enrich human life. For the pluralist, the choice between Plato's absolutism and moral relativism is a false dichotomy. Just because there is no absolute "good" does not mean that all goods or values are relative to the time, place, and culture in which we find them. Some things and practices are usually bad for humans, others are usually good, and the discovery and encouragement of the good things and practices is the game the smart ethicist plays.

For this reason, pluralists emphasize the importance of investigating and questioning. Is our present culture enhancing or diminishing us as human beings? Is the American attitude toward sexuality, say, improving the human condition or interfering with it? (And before we can answer that question, what *is* the American attitude toward sexuality? Or are there many attitudes?) The ethical contribution to the history of philosophy made by the fascinating twentieth-century movement called *existentialism* is its insistence on this kind of vigorous, ruthlessly honest interrogation of oneself and one's culture. The danger of hypocrisy and self-deception, or what the leading existentialist **Jean-Paul Sartre (1912–1984)** called *bad faith*, is rampant in every culture: challenging our values is uncomfortable. It is much easier for us, like the subjects of the nude ruler in H. C. Andersen's fable *The Emperor's New Clothes*, to collectively pretend that something is good (even if we know there is really nothing there at all). Thus, the project of becoming a good person becomes not just a matter of following the rules, doing one's duty, seeking happiness, becoming virtuous, or caring for others. It is also the lifelong project of discovering *if*, *when*, *and why* the apparently good things we seek are what we ought to pursue.

SUMMARY

After reading this appendix, a reasonable student might ask: "But which of these moralities is the *right* one?" Admittedly, philosophers are better at posing problems than solving them. But the lesson was not in demonstrating that one or another morality is the one a person ought to follow. Rather, this appendix has attempted to show you how different people have struggled with the enormously difficult questions of ethics. Many people think they simply know the difference between right and wrong, or unreflectively accept the definitions of right and wrong offered by their parents, churches, communities, or societies. This appendix tried to show that there is nothing simple about ethics. To understand ethics means to think, to challenge, to question, and to reflect. Accordingly, being a good person might mean attempting your own struggle with, and attempting to find your own answer to, what we called Plato's knotty question of goodness.

GLOSSARY

acceptable use policy (AUP) A document that stipulates restrictions and practices that a user must agree in order to use organizational computing and network resources.

acceptance When an organization decides to accept a risk because the cost of avoiding the risk outweighs the potential loss of the risk. A decision to accept a risk can be extremely difficult and controversial when dealing with safety-critical systems because making that determination involves forming personal judgments about the value of human life, assessing potential liability in case of an accident, evaluating the potential impact on the surrounding natural environment, and estimating the system's costs and benefits.

advanced persistent threat (APT) A network attack in which an intruder gains access to a network and stays there—undetected—with the intention of stealing data over a long period of time (weeks or even months).

agile development A software development methodology in which a system is developed in iterations lasting from one to four weeks. Unlike the waterfall system development model, agile development accepts the fact that system requirements are evolving and cannot be fully understood or defined at the start of the project.

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) An agreement of the World Trade Organization that requires member governments to ensure that intellectual property rights can be enforced under their laws and that penalties for infringement are tough enough to deter further violations.

American Recovery and Reinvestment Act A wide-ranging act that authorized $787 billion in spending and tax cuts over a 10-year period and included strong privacy provisions for electronic health records, such as banning the sale of health information, promoting the use of audit trails and encryption, and providing rights of access for patients.

annualized loss expectancy (ALE) The estimated loss from a potential risk event over the course of a year. The following equation is used to calculate the annual loss expectancy: ARO × SLE = ALE. Where ARO is the annualized rate of occurrence, an estimate of the probability that this event will occur over the course of a year and SLE is the single loss expectancy, the estimated loss that would be incurred if the event happens.

annualized rate of occurrence (ARO) An estimate of the probability that a risk event will occur over the course of a year.

anonymous expression The expression of opinions by people who do not reveal their identity.

anonymous remailer service A service that allows anonymity on the Internet by using a computer program that strips the originating header and/or IP address from the message and then forwards the message to its intended recipient.

anti-SLAPP laws Laws designed to reduce frivolous SLAPPs (strategic lawsuit against public participation (SLAPP), which is a lawsuit filed by corporations, government officials, and others against citizens and community groups who oppose them on matters of concern).

antivirus software Software that scans for a specific sequence of bytes, known as a virus signature, that indicates the presence of a specific virus.

artificial intelligence systems The people, procedures, hardware, software, data, and knowledge needed to develop computer systems and machines that can simulate human intelligence processes, including learning (the acquisition of information and rules for using the information), reasoning (using rules to reach conclusions), and self-correction (using the outcome from one scenario to improve its performance on future scenarios).

audit committee A group that provides assistance to the board of directors in fulfilling its responsibilities with respect to the oversight of the quality and integrity of the organization's accounting and reporting practices and controls, including financial statements and reports; the organization's compliance with legal and regulatory requirements; the qualifications, independence, and performance of the company's independent auditor; and the performance of the company's internal audit team.

avoidance The elimination of a vulnerability that gives rise to a particular risk in order to avoid the risk altogether. This is the most effective solution but often not possible due to organizational requirements and factors beyond an organization's control.

Bathsheba syndrome The moral corruption of people in power, which is often facilitated by a tendency for people to look the other way when their leaders act inappropriately.

best practice A method or technique that has consistently shown results superior to those achieved with other means and that is used as a benchmark within a particular industry.

Bill of Rights The first 10 amendments to the United States Constitution that spell out additional rights of individuals.

black-box testing A type of dynamic testing that involves viewing the software unit as a device that has expected input and output behaviors but whose internal workings are unknown (a black box).

blended threat A sophisticated threat that combines the features of a virus, worm, Trojan horse, and other malicious code into a single payload.

body of knowledge An agreed-upon sets of skills and abilities that all licensed professionals must possess.

botnet A large group of computers, which are controlled from one or more remote locations by hackers, without the knowledge or consent of their owners.

breach of contract The failure of one party to meet the terms of a contract.

breach of the duty of care The failure to act as a reasonable person would act.

breach of warranty When a product fails to meet the terms of its warranty.

bribery The act of providing money, property, or favors to someone in business or government in order to obtain a business advantage.

bring your own device (BYOD) A business policy that permits, and in some cases, encourages employees to use their own mobile devices (smartphones, tablets, or laptops) to access company computing resources and applications, including email, corporate databases, the corporate intranet, and the Internet.

BSA | The Software Alliance A trade group that represent the world's largest software and hardware manufacturers.

business continuity plan A risk-based strategy that includes an occupant emergency evacuation plan, a continuity of operations plan, and an incident management plan with an active governance process to minimize the potential impact of any security incident and to ensure business continuity in the event of a cyberattack or some form of disaster.

business information system A set of interrelated components—including hardware, software, databases, networks, people, and procedures—that collects and processes data and disseminates the output.

Capability Maturity Model Integration (CMMI) models Collection of best practices that help organizations improve their processes.

CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) Software that generates and grades tests that humans can pass and all but the most sophisticated computer programs cannot.

certification Indicates that a professional possesses a particular set of skills, knowledge, or abilities, in the opinion of the certifying organization. Certification can also apply to products (e.g., the Wi-Fi CERTIFIED logo assures that the product has met rigorous interoperability testing to ensure that it will work with other Wi-Fi-certified products) and is generally voluntary.

Child Online Protection Act (COPA) An act signed into law in 1998 with the aim of prohibiting the making of harmful material available to minors via the Internet; the law was ultimately ruled largely unconstitutional.

Children's Internet Protection Act (CIPA) An act passed in 2000; it required federally financed schools and libraries to use some form of technological protection (such as an Internet filter) to block computer access to obscene material, pornography, and anything else considered harmful to minors.

Children's Online Privacy Protection Act (COPPA) An act implemented in 1998 in an attempt to give parents control over the collection, use, and disclosure of their children's personal information.

CIA security triad Refers to confidentiality, integrity, and availability.

clinical decision support (CDS) A process and a set of tools designed to enhance healthcare-related decision making through the use of clinical knowledge and patient-specific information to improve healthcare delivery.

CMMI-Development (CMMI-DEV) A specific application of CMMI frequently used to assess and improve software development practices.

code of ethics A statement that highlights an organization's key ethical issues and identifies the overarching values and principles that are important to the organization and its decision making.

coemployment relationship A employment situation in which two employers have actual or potential legal rights and duties with respect to the same employee or group of employees.

Communications Assistance for Law Enforcement Act (CALEA) An act passed in 1994 that amended the Wiretap Act and Electronic Communications Privacy Act, which required the telecommunications industry to build tools into its products that federal investigators could use—after obtaining a court order—to eavesdrop on conversations and intercept electronic communications.

Communications Decency Act (CDA) Title V of the Telecommunications Act, it aimed at protecting children from pornography, including imposing $250,000 fines and prison terms of up to two years for the transmission of "indecent" material over the Internet.

compliance To be in accordance with established policies, guidelines, specifications, or legislation.

computer forensics A discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law.

computerized provider order entry (CPOE) system A system that enables physicians to place orders (for drugs, laboratory tests, radiology, physical therapy) electronically, with the orders transmitted directly to the recipient.

conflict of interest A conflict between a person's (or firm's) self-interest and the interests of a client.

contingent work A job situation in which an individual does not have an explicit or implicit contract for long-term employment.

contributory negligence When the plaintiffs' own actions contributed to their injuries.

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act A law that specifies that it is legal to spam, provided the messages meet a few basic requirements—spammers cannot disguise their identity by using a false return address, the email must include a label specifying that it is an ad or a solicitation, and the email must include a way for recipients to indicate that they do not want future mass mailings.

cookie Text files that can be downloaded to the hard drives of users who visit a website, so that the website is able to identify visitors on subsequent visits.

copyright The exclusive right to distribute, display, perform, or reproduce an original work in copies or to prepare derivative works based on the work; granted to creators of original works of authorship.

copyright infringement A violation of the rights secured by the owner of a copyright; occurs when someone copies a substantial and material part of another's copyrighted work without permission.

corporate compliance officer *See* corporate ethics officer.

corporate ethics officer A senior-level manager who provides an organization with vision and leadership in the area of business conduct.

corporate social responsibility (CSR) The concept that an organization should act ethically by taking responsibility for the impact of its actions on its shareholders, consumers, employees, community, environment, and suppliers.

cost per click (CPC) One of the two common methods of charging for paid media, where ads are paid for only when someone actually clicks on them.

cost per thousand impressions (CPM) One of the two common methods of charging for paid media, where ads are billed at a flat rate per 1,000 impressions, which is a measure of the number of times an ad is displayed—whether it was actually clicked on or not.

cyberabuse Any form of mistreatment or lack of care, both physical and mental, based on the use of an electronic communications device that causes harm and distress to others.

cyberespionage The deployment of malware that secretly steals data in the computer systems of organizations, such as government agencies, military contractors, political organizations, and manufacturing firms.

cyberharassment A form of cyberabuse in which the abusive behavior, which involves the use of an electronic communications device, is degrading, humiliating, hurtful, insulting, intimidating, malicious, or otherwise offensive to an individual or group of individuals causing substantial emotional distress.

cyberloafing Using the Internet for purposes unrelated to work such as posting to Facebook, sending personal emails or Instant messages, or shopping online.

cybersquatter A person or company that registers domain names for famous trademarks or company names to which they have no connection, with the hope that the trademark's owner will buy the domain name for a large sum of money.

cyberstalking Threatening behavior or unwanted advances directed at an adult using the Internet or other forms of online and electronic communications; the adult version of cyberbullying.

cyberterrorism The intimidation of government or civilian population by using information technology to disable critical national infrastructure (e.g., energy, transportation, financial, law enforcement, and emergency response) to achieve political, religious, or ideological goals.

decision support system (DSS) A type of business information system used to improve decision making in a variety of industries.

defamation Making either an oral or a written statement of alleged fact that is false and that harms another person.

Defend Trade Secrets Act of 2016 An act passed in 2016 that amended the Economic Espionage Act to create a federal civil remedy for trade secret misappropriation.

deliverable Products created during various stages of the development process, including statements of requirements, flowcharts, and user documentation.

Department of Homeland Security (DHS) A large federal agency with more than 240,000 employees and a budget of almost $65 billion whose goal is to provide for a "safer, more secure America, which is resilient against terrorism and other potential threats."

design patent A type of patent that permits its owner to exclude others from making, using, or selling the design in question.

Digital Millennium Copyright Act (DMCA) Signed into law in 1998, the act addresses a number of copyright-related issues, with Title II of the act providing limitations on the liability of an Internet service provider for copyright infringement.

disaster recovery plan A documented process for recovering an organization's business information system assets—including hardware, software, data, networks, and facilities—in the event of a disaster.

distributed denial-of-service (DDoS) attack An attack in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks.

Doxing Doing research on the Internet to obtain someone's private personal information—such as home address, email address, phone numbers, and place of employment—and even private electronic documents, such as photographs, and then posting that information online without permission.

duty of care The obligation to protect people against any unreasonable harm or risk.

dynamic testing A QA process that tests the code for a completed unit of software by actually entering test data and comparing the results to the expected results.

earned media Media exposure an organization gets through press and social media mentions, positive online ratings, reviews, tweets and retweets, reposts (or "shares"), recommendations, and so on.

Economic Espionage Act (EEA) of 1996 An act passed in 1996 to help law enforcement agencies pursue economic espionage. It imposes penalties of up to $10 million and 15 years in prison for the theft of trade secrets.

Electronic Communications Privacy Act (ECPA) An act that deals with the protection of three main issues: (1) the protection of communications while in transfer from sender to receiver; (2) the protection of communications held in electronic storage; and (3) the prohibition of devices from recording dialing, routing, addressing, and signaling information without a search warrant.

electronic discovery (e-discovery) The collection, preparation, review, and production of electronically stored information for use in criminal and civil actions and proceedings.

electronic health record (EHR) A comprehensive view of the patient's complete medical history designed to be shared with authorized providers and staff from more than one organization.

electronic medical record (EMR) A collection of health-related information on an individual that is created, managed, and consulted by authorized clinicians and staff within a single healthcare organization.

Electronic Product Environmental Assessment Tool (EPEAT) A system that enables purchasers to evaluate, compare, and select electronic products based on a total of 51 environmental criteria.

electronically stored information (ESI) Any form of digital information, including emails, drawings, graphs, web pages, photographs, word-processing files, sound recordings, and databases stored on any form of magnetic storage device, including hard drives, CDs, and flash drives.

employee leasing A business arrangement in which an organization (called the subscribing firm) transfers all or part of its workforce to another firm (called the leasing firm), which handles all human resource-related activities and costs, such as payroll, training, and the administration of employee benefits. The subscribing firm leases these workers to an organization, but they remain employees of the leasing firm.

encryption The process of scrambling messages or data in such a way that only authorized parties can read it.

encryption key A value that is applied (using an algorithm) to a set of unencrypted text (plaintext) to produce encrypted text that appears as a series of seemingly random characters (ciphertext) that is unreadable by those without the encryption key needed to decipher it.

ethics A code of behavior that is defined by the group to which an individual belongs.

European Union Data Protection Directive A directive that requires any company doing business within the borders of the countries comprising the European Union (EU) to implement a set of privacy directives on the fair and appropriate use of information.

exploit An attack on an information system that takes advantage of a particular system vulnerability.

failure mode A description of how a product or process could fail to perform the desired functions described by the customer.

failure mode and effects analysis (FMEA) An important technique used to develop ISO 9000-compliant quality systems by both evaluating reliability and determining the effects of system and equipment failures.

Fair and Accurate Credit Transactions Act An amendment to the Fair Credit Reporting Act passed in 2003 that allows consumers to request and obtain a free credit report once each year from each of the three primary consumer credit reporting companies (Equifax, Experian, and TransUnion).

Fair Credit Reporting Act An act that regulates the operations of credit-reporting bureaus, including how they collect, store, and use credit information.

fair information practices A term for a set of guidelines that govern the collection and use of personal data.

fair use doctrine A legal doctrine that allows portions of copyrighted materials to be used without permission under certain circumstances. Title 17, section 107, of the U.S. Code established the following four factors that courts should consider when deciding whether a particular use of copyrighted property is fair and can be allowed without penalty: (1) the purpose and character of the use (such as commercial use or nonprofit, educational purposes), (2) the nature of the copyrighted work, (3) the portion of the copyrighted work used in relation to the work as a whole, and (4) the effect of the use on the value of the copyrighted work.

False Claims Act A law enacted during the U.S. Civil War to combat fraud by companies that sold supplies to the Union Army; also known as the Lincoln Law. *See also* qui tam.

Family Educational Rights and Privacy Act (FERPA) A federal law that assigns certain rights to parents regarding their children's educational records.

firewall Hardware or software (or a combination of both) that serves as the first line of defense between an organization's network and the Internet; a firewall also limits access to the company's network based on the organization's Internet-usage policy.

First Amendment The first amendment in the U.S. Constitution that protects Americans' rights to freedom of religion, freedom of expression, and freedom to assemble peaceably.

Foreign Corrupt Practices Act (FCPA) An act that makes it a crime to bribe a foreign official, a foreign political party official, or a candidate for foreign political office.

foreign intelligence Information relating to the capabilities, intentions, or activities of foreign governments or agents of foreign governments or foreign organizations.

Foreign Intelligence Surveillance Act (FISA) Describes procedures for the electronic surveillance and collection of foreign intelligence information in communication between foreign powers and the agents of foreign powers.

Foreign Intelligence Surveillance Act (FISA) Court Created by the FISA, this court meets in secret to hear applications for orders approving electronic surveillance anywhere within the United States.

Foreign Intelligence Surveillance Amendments Act of 2008 An act that granted NSA expanded authority to collect, without court-approved warrants, international communications as they flow through U.S. telecommunications network equipment and facilities.

Fourth Amendment An amendment to the United States Constitution that protects citizens from unreasonable government searches and is often invoked to protect the privacy of government employees.

fraud The crime of obtaining goods, services, or property through deception or trickery.

Freedom of Information Act (FOIA) A law that grants citizens the right to access certain information and records of federal, state, and local governments upon request.

gig economy A work environment in which temporary positions are common and organizations contract with independent workers for short-term engagements.

government license A government-issued permission to engage in an activity or to operate a business.

Gramm-Leach-Bliley Act (GLBA) A bank deregulation law that repealed a Depression-era law known as Glass–Steagall and requires companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data.

green computing Efforts directed toward the efficient design, manufacture, operation, and disposal of IT-related products, including personal computers, laptops, servers, printers, and printer supplies.

H-1B visa A temporary work visa granted by the U.S. Citizenship and Immigration Services (USGIS) for people who work in specialty occupations—jobs that require a four-year bachelor's degree in a specific field, or equivalent experience.

hate speech Persistent or malicious harassment aimed at a specific person that can be prosecuted under the law.

hazard log A logging and monitoring system used by safety engineers to track hazards from a project's start to its finish.

health information exchange (HIE) The process of sharing patient-level electronic health information between different organizations.

Health Information Technology for Economic and Clinical Health Act (HITECH) A program to incentivize physicians and hospitals to implement such systems. Under this act, increased Medicaid and Medicare reimbursements are made to doctors and hospitals that demonstrate "meaningful use" of electronic health record (EHR) technology.

Health Insurance Portability and Accountability Act (HIPAA) An act designed to improve the portability and continuity of health insurance coverage; to reduce fraud, waste, and abuse in health insurance and healthcare delivery; and to simplify the administration of health insurance.

high-quality software system Systems that are easy to learn and use because they perform quickly and efficiently; they meet their users' needs; and they operate safely and reliably so that system downtime is kept to a minimum.

identity theft The theft of personal information, which is then used without the owner's permission.

independent contractor An individual who provides services to another individual or organization according to terms defined in a written contract or within a verbal agreement.

industrial espionage The use of illegal means to obtain business information not available to the general public.

information privacy The combination of communications privacy and data privacy.

information security (infosec) group A group within an organization managing the processes, tools, and policies necessary to prevent, detect, document, and counter threats to digital and nondigital information, whether it is in transit, being processed, or at rest in storage.

integration testing Software testing done after successful unit testing, where the software units are combined into an integrated subsystem that undergoes rigorous testing to ensure that the linkages among the various subsystems work successfully.

integrity Adherence to a personal code of principles.

intellectual property Works of the mind—such as art, books, films, formulas, inventions, music, and processes—that are distinct and owned or created by a single person or group. Intellectual property is protected through copyright, patent, trade secret, and trademark laws.

internal control The process established by an organization's board of directors, managers, and IT systems people to provide reasonable assurance for the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations.

Internet censorship The control or suppression of the publishing or accessing of information on the Internet.

Internet filter Software that can be used to block access to certain websites that contain material deemed inappropriate or offensive.

intrusion detection system (IDS) Software and/or hardware that monitors system and network resources and activities and notifies network security personnel when it detects network traffic that attempts to circumvent the security measures of a networked computer environment.

ISAE No. 3402 Developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organizations and their auditors (user auditors) on the controls at a service organization that are likely to impact or be a part of the user organization's system of internal control over financial reporting. The international counterpart to SSAE No. 16. *See also* SSAE No. 16 audit report.

ISO 9001 family of standards A set of standards written to serve as a guide to quality products, services, and management. It provides a set of standardized requirements for a quality management system.

IT user A person who uses a hardware or software product; the term distinguishes end users from the IT workers who develop, install, service, and support the product. IT users need the product to deliver organizational benefits or to increase their productivity.

John Doe lawsuit A type of lawsuit that organizations may file in order to gain subpoena power in an effort to learn the identity of anonymous Internet users who they believe have caused some form of harm to the organization through their postings.

labor productivity A measure of economic performance that compares the amount of goods and services produced (output) with the number of labor hours used in producing those goods and services.

law A system of rules that tells us what we can and cannot do.

Leahy-Smith America Invents Act An act that changed the U.S. patent system so that the first person to file with the U.S. Patent and Trademark Office will receive the patent, not necessarily the person who actually invented the item first.

libel A written defamatory statement.

litigation hold notice Instructions sent by organizations to inform its employees (or employees of the opposing party) to save relevant data and to suspend data that might be due to be destroyed based on normal data-retention rules.

live telemedicine A form of telemedicine in which patients and healthcare providers are present at different sites at the same time; often involves a videoconference link between the two sites.

logic bomb A type of Trojan horse malware that executes when it is triggered by a specific event or at a predetermined time.

machine learning A type of artificial intelligence (AI), involves computer programs that can learn some task and improve their performance with experience.

managed security service provider (MSSP) A company that monitors, manages, and maintains computer and network security for other organizations.

material breach of contract The failure of one party to perform certain expressed or implied obligations, which impairs or destroys the essence of the contract.

misrepresentation The misstatement or incomplete statement of a material fact.

mission-critical process Business processes that are more pivotal to continued operations and goal attainment than others.

mitigation The reduction in either the likelihood or the impact of the occurrence of a risk.

morals The personal principles upon which an individual bases his or her decisions about what is right and what is wrong.

National Security Letter (NSL) Compels holders of your personal records to turn them over to the government; an NSL is not subject to judicial review or oversight.

natural language processing An aspect of artificial intelligence that involves technology that allows computers to understand, analyze, manipulate, and/or generate "natural" languages, such as English.

negligence Not doing something that a reasonable person would do or doing something that a reasonable person would not do.

next-generation firewall (NGFW) A hardware- or software-based network security system that is able to detect and block sophisticated attacks by filtering network traffic dependent on the packet contents.

noncompete agreement Terms of an employment contract that prohibit an employee from working for any competitors for a specified period of time, often one to two years.

nondisclosure clauses Terms of an employment contract that prohibit an employee from revealing secrets.

NSL gag provision Prohibits National Security Letter (NSL) recipients from informing anyone, even the person who is the subject of the NSL request, that the government has secretly requested his or her records.

N-version programming An approach to minimizing the impact of software errors by independently implementing the same set of user requirements N times (where N could be 2, 3, 4 or more); the N-versions of software are run in parallel; and, if a difference is found, a "voting algorithm" is executed to determine which result to use.

offshore outsourcing A form of outsourcing in which services are provided by an organization whose employees are in a foreign country.

open source code Any program whose source code is made available for use or modification, as users or other developers see fit.

opt in To give an organization the right to share personal data, such as annual earnings, net worth, employers, personal investment information, loan amounts, and Social Security numbers, to other organizations.

opt out To refuse to give an organization the right to collect and share personal data with unaffiliated parties.

organic media marketing A form of marketing that employs tools provided by or tailored for a particular social media platform to build a social community and interact with it by sharing posts and responding to customer comments on the organization's blog and social media accounts.

outsourcing A long-term business arrangement in which a company contracts for services with an outside organization that has expertise in providing a specific function.

paid media marketing A form of marketing that involves paying a third party to broadcast an organization's display ads or sponsored messages to social media users.

patent A grant of a property right issued by the U.S. Patent and Trademark Office to an inventor; permits its owner to exclude the public from making, using, or selling a protected invention, and allows for legal action against violators.

patent infringement A violation of the rights secured by the owner of a patent; occurs when someone makes unauthorized use of another's patent.

PATRIOT Sunsets Extension Act of 2011 An act that granted a four-year extension of two key provisions in the USA PATRIOT Act that allowed roving wiretaps and searches of business records.

pen register A device that records electronic impulses to identify the numbers dialed for outgoing calls.

personal health record (PHR) Information from the electronic health record (EHR) that are routinely shared with the patient—such as personal identifiers, contact information, health provider information, problem list, medication history, allergies, immunizations, and lab and test results.

phishing The act of fraudulently using email to try to get the recipient to reveal personal data.

plagiarism The act of stealing someone's ideas or words and passing them off as one's own.

policy The guidelines and standards by which the organization must abide.

predictive coding A process that couples human guidance with computer-driven concept searching in order to "train" document review software to recognize relevant documents within a large collection of documents.

prior art The existing body of knowledge that is available to a person of ordinary skill in the art.

Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008 An act that created the position of Intellectual Property Enforcement Coordinator within the Executive Office of the President. It also increased trademark and copyright enforcement and substantially increased penalties for infringement.

Privacy Act Establishes a code of fair information practices that sets rules for the collection, maintenance, use, and dissemination of personal data that is kept in systems of records by federal agencies.

problem statement A clear, concise description of the issue that needs to be addressed.

procedure Defines the exact instructions for completing each task in a process.

process A collection of tasks designed to accomplish a stated objective.

product liability The liability of manufacturers, sellers, lessors, and others for injuries caused by defective products.

professional code of ethics The principles and core values that are essential to the work of a particular occupational group.

professional employer organization (PEO) A business entity that coemploys the employees of its clients and typically assumes responsibility for all human resource management functions.

professional malpractice Breach of the duty of care by a professional.

quality assurance (QA) Methods within the development process that are designed to guarantee reliable operation of a product.

quality management The defining, measuring, and refining of the quality of the development process and the products developed during its various stages. The objective of quality management is to help developers deliver high-quality systems that meet the needs of their users.

qui tam A provision of the False Claims Act that allows a private citizen to file a suit in the name of the U.S. government, charging fraud by government contractors and other entities who receive or use government funds. *See also* False Claim Act.

ransomware Malware that stops you from using your computer or accessing your data until you meet certain demands, such as paying a ransom or sending photos to the attacker.

reasonable assurance A concept in computer security that recognizes that managers must use their judgment to ensure that the cost of control does not exceed the system's benefits or the risks involved.

reasonable person standard A legal standard that defines how an objective, careful, and conscientious person would have acted in the same circumstances.

reasonable professional standard A legal standard that defendants who have particular expertise or competence are measured against.

redundancy The provision of multiple interchangeable components to perform a single function in order to cope with failures and errors.

reliability A measure of the rate of failure in a system that would render it unusable over its expected lifetime.

remote monitoring Also called home monitoring, it is the regular, ongoing, accurate measurement of an individual's vital signs (temperature, blood pressure, heart rate, and breathing rate) and other health measures (e.g., glucose levels for a diabetic) and the transmission of this data to a healthcare provider.

résumé inflation Falsely claiming competence in a skill, usually because that skill is in high demand.

reverse engineering The process of taking something apart in order to understand it, build a copy of it, or improve it.

right of privacy "the right to be left alone—the most comprehensive of rights, and the right most valued by a free people."

Right to Financial Privacy Act An act that protects the records of financial institution customers from unauthorized scrutiny by the federal government.

risk assessment The process of assessing security-related risks to an organization's computers and networks from both internal and external threats.

risk The potential of gaining or losing something of value. Risk can be quantified by three elements: a risk event, the probability of the event happening, and the impact (positive or negative) on the business outcome if the risk does actually occur.

risk management The process of identifying, monitoring, and limiting risks to a level that an organization is willing to accept.

robotics A branch of engineering that involves the development and manufacture of mechanical or computer devices that can perform tasks that require a high degree of precision or that are tedious or hazardous for human beings, such as painting cars or making precision welds.

rootkit A set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge.

safety-critical system A system whose failure may cause human injury or death.

Section 230 of the CDA A section of the Communications Decency Act that provides immunity to an Internet service provider (ISP) that publishes user-generated content, as long as its actions do not rise to the level of a content provider.

security audit An evaluation of whether an organization has a well-considered security policy in place and if it is being followed.

security policy An organization's security requirements, as well as the controls and sanctions needed to meet those requirements.

separation of duties The concept of having different aspects of a process handled by different people to prevent fraud.

sexting Sending sexual messages, nude or seminude photos, or sexually explicit videos over a cell phone.

single loss expectancy (SLE) The estimated loss that would be incurred if a risk event occurs.

slander An oral defamatory statement.

smishing Another variation of phishing that involves the use of texting.

social audit A process whereby an organization reviews how well it is meeting its ethical and social responsibility goals and communicates its new goals for the upcoming year.

social media Web-based communication channels and tools that enable people to interact with each other by creating online communities where they can share information, ideas, messages, and other content, including images, audio, and video.

social media marketing A form of marketing that involves the use of social networks to communicate and promote the benefits of products and services.

social networking platform Technology that allows creation of an online community of Internet users that enables members to break down barriers created by time, distance, and cultural differences.

social shopping platform A combination of shopping and social networking.

Software & Information Industry Association (SIIA) A trade group that represents the world's largest software and hardware manufacturers.

software defect Any error that, if not removed, could cause a software system to fail to meet its users' needs.

software development methodology A standard, proven work process that enables systems analysts, programmers, project managers, and others to make controlled and orderly progress in developing high-quality software.

software engineer One who applies engineering principles and practices to the design, development, implementation, testing, and maintenance of software.

software piracy A form of copyright infringement that involves making copies of software or enabling others to access software to which they are not entitled.

software quality The degree to which a software product meets the needs of its users.

spam The use of email systems to send unsolicited email to large numbers of people.

spear phishing A variation of phishing in which the phisher sends fraudulent emails to a certain organization's employees.

SSAE No. 16 audit report An auditing standard issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). It demonstrates that an outsourcing firm has effective internal controls in accordance with the Sarbanes-Oxley Act of 2002.

stakeholder Someone who stands to gain or lose, depending on how a particular situation is resolved.

stalking app A cell phone spy software that can be loaded onto someone's cell phone or smartphone within minutes, making it possible for the user to perform location tracking, record calls, view every text message or picture sent or received, and record the URLs of any website visited on the phone.

static testing A software-testing technique in which software is tested without actually executing the code. It consists of two steps—review and static analysis.

store-and-forward telemedicine The acquiring of data, sound, images, and video from a patient and then transmitting everything to a medical specialist for later evaluation.

strategic lawsuit against public participation (SLAPP) A lawsuit filed by corporations, government officials, and others against citizens and community groups who oppose them on matters of concern. The lawsuit is typically without merit and is used to intimidate critics out of fear of the cost and effort associated with a major legal battle.

strict liability A situation in which the defendant is held responsible for injuring another person, regardless of negligence or intent.

supply chain sustainability A component of corporate social responsibility (CSR) that focuses on developing and maintaining a supply chain that meets the needs of the present without compromising the ability of future generations to meet their needs.

system safety engineer Someone who has explicit responsibility for ensuring that a system will operate in a safe and reliable manner while meeting its users' needs.

system testing Software testing done after successful integration testing, where the various subsystems are combined to test the entire system as a complete entity.

telehealth Employs electronic information processing and telecommunications to support at-a-distance health care, provide professional and patient health-related training, and support healthcare administration.

telemedicine A component of telehealth that provides medical care to people at a location different from the healthcare providers.

Title III of the Omnibus Crime Control and Safe Streets Act A law that regulates the interception of wire (telephone) and oral communications; also known as the Wiretap Act.

trade secret Information, generally unknown to the public, that a company has taken strong measures to keep confidential.

trademark A logo, package design, phrase, sound, or word that enables a consumer to differentiate one company's products from another's.

transborder data flow The flow of personal data across national boundaries.

transference A risk management strategy in which the risk, should it happen, does not rest solely on one individual or organization. For example, a common way to accomplish risk transference is for an individual or an organization to purchase insurance, such as auto or business liability insurance. Another way to transfer risk is to outsource the risk by contracting with a third party to manage the risk.

Transport Layer Security (TLS) A communications protocol or system of rules that ensures privacy between communicating applications and their users on the Internet.

trap and trace A device that records the originating number of incoming calls for a particular phone number.

Trojan horse A seemingly harmless program in which malicious code is hidden.

U.S. Computer Emergency Readiness Team (US-CERT) Established in 2003 to protect the nation's Internet infrastructure against cyberattacks, it serves as a clearinghouse for information on new viruses, worms, and other computer security topics.

U.S. person Under FISA, it is defined as a U.S. citizen, permanent resident, or company.

Uniform Trade Secrets Act (UTSA) An act drafted in the 1970s to bring uniformity to all the United States in the area of trade secret law.

unit testing A software-testing technique that involves testing individual components of code (subroutines, modules, and programs) to verify that each unit performs as intended.

USA Freedom Act An act passed following startling revelations by Edward Snowden of secret NSA surveillance programs, which terminated the bulk collection of telephone metadata by the NSA.

USA PATRIOT Act An act passed 5 weeks after the terrorist attacks of September 11, 2001. It gave sweeping new powers both to domestic law enforcement and U.S. international intelligence agencies, including increasing the ability of law enforcement agencies to search telephone, email, medical, financial, and other records.

user acceptance testing Software testing done independently by trained end users to ensure the system operates as expected.

utility patent A type of patent "issued for the invention of a new and useful process, machine, manufacture, or composition of matter, or a new and useful improvement thereof, it generally permits its owner to exclude others from making, using, or selling the invention for a period of up to 20 years from the date of patent application filing, subject to the payment of maintenance fees."

vehicle event data recorder (EDR) A device that records vehicle and occupant data for a few seconds before, during, and after any vehicle crash that is severe enough to deploy the vehicle's air bags.

vice A habit of unacceptable behavior.

viral marketing An approach to advertising that encourages individuals to pass along a marketing message to others, thus creating the potential for exponential growth in the message's exposure and influence.

virtue A habit that inclines people to do what is acceptable.

virus A piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner.

virus signature A specific sequence of bytes that indicates to antivirus software that a specific virus is present.

vishing Similar to smishing except that the victims receive a voice-mail message telling them to call a phone number or access a website.

warranty Assures buyers or lessees that a product meets certain standards of quality.

waterfall system development model A software development methodology that involves a sequential, multistage system development process in which development of the next stage of the system cannot begin until the results of the current stage are approved or modified as necessary.

whistle-blowing An effort by an employee to attract attention to a negligent, illegal, unethical, abusive, or dangerous act by a company that threatens the public interest.

white-box testing A type of dynamic testing that treats the software unit as a device that has expected input and output behaviors but whose internal workings, unlike the unit in black-box testing, are known.

Wiretap Act A law that regulates the interception of wire (telephone) and oral communications; also known as the Title III of the Omnibus Crime Control and Safe Streets Act.

worm A harmful program that resides in the active memory of the computer and duplicates itself.

zero-day exploit A cyberattack that takes place before the security community and/or software developers become aware of and fix a security vulnerability.

zombie A computer that is part of a botnet and that is controlled by a hacker without the knowledge or consent of the owner.

INDEX