ETHICS IN INFORMATION TECHNOLOGY

George W. Reynolds

ETHICS IN INFORMATION TECHNOLOGY

Fifth Edition

ETHICS IN INFORMATION TECHNOLOGY

Fifth Edition

George W. Reynolds
Strayer University

CENGAGE Learning®

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

CENGAGE Learning®

Ethics in Information Technology, Fifth Edition
George W. Reynolds

Product Director: Joe Sabatino

Product Manager: Clara Goosman

Senior Content Developer: Kate Mason

Product Assistant: Brad Sullender

Senior Rights Acquisitions Specialist: Christine Myaskovsky

Senior Brand Manager: Robin LeFevre

Art and Cover Direction, Production Management, and Composition: PreMediaGlobal

Associate Market Development Manager: Roy Rosa

Marketing Coordinator: Christopher Walz

Senior Media Developer: Mike Jackson

Manufacturing Planner: Ron Montgomery

Cover Images: © Paul Price/Ikon Images/ Getty Images.

Library of Congress Control Number: 2013945101

ISBN-13: 978-1-285-19715-9

ISBN-10: 1-285-19715-1

Instructor Edition:

ISBN-13: 978-1-285-19718-0

ISBN-10: 1-285-19718-6

Cengage Learning
20 Channel Center Street
Boston, MA 02210
USA

Printed in the United States of America
1 2 3 4 5 6 7 17 16 15 14 13

BRIEF CONTENTS

Preface			xiii
Chapter	**1**	*An Overview of Ethics*	1
Chapter	**2**	*Ethics for IT Workers and IT Users*	41
Chapter	**3**	*Computer and Internet Crime*	81
Chapter	**4**	*Privacy*	131
Chapter	**5**	*Freedom of Expression*	179
Chapter	**6**	*Intellectual Property*	217
Chapter	**7**	*Software Development*	261
Chapter	**8**	*The Impact of Information Technology on Productivity and Quality of Life*	297
Chapter	**9**	*Social Networking*	335
Chapter	**10**	*Ethics of IT Organizations*	369
Appendix A		*A Brief Introduction to Morality*	411
Appendix B		*Answers to Self-Assessment Questions*	427
Glossary			429
Index			441

TABLE OF CONTENTS

Preface xiii

Chapter 1 *An Overview of Ethics* 1
- Vignette 1
  - Cisco Chairman and CEO Advocates Ethical Behavior 1
- What Is Ethics? 3
  - Definition of Ethics 3
  - The Importance of Integrity 4
  - The Difference Between Morals, Ethics, and Laws 5
- Ethics in the Business World 5
  - Corporate Social Responsibility 8
  - Why Fostering Corporate Social Responsibility and Good Business Ethics Is Important 8
  - Improving Corporate Ethics 12
  - Creating an Ethical Work Environment 18
- Including Ethical Considerations in Decision Making 20
  - Develop a Problem Statement 21
  - Identify Alternatives 21
  - Evaluate and Choose an Alternative 22
  - Implement the Decision 24
  - Evaluate the Results 24
- Ethics in Information Technology 24
- Summary 26
- Key Terms 27
- Self-Assessment Questions 27
- Discussion Questions 28
- What Would You Do? 29
- Cases 31
- End Notes 35

Chapter 2 *Ethics for IT Workers and IT Users* 41
- Vignette 41
  - New York City Payroll Project Riddled with Fraud 41
- IT Professionals 43
  - Are IT Workers Professionals? 44
  - Professional Relationships That Must Be Managed 44
  - Professional Codes of Ethics 54
  - Professional Organizations 55
  - Certification 57

Government Licensing 58
IT Professional Malpractice 60
IT Users 61
Common Ethical Issues for IT Users 61
Supporting the Ethical Practices of IT Users 63
Compliance 64
Summary 67
Key Terms 68
Self-Assessment Questions 68
Discussion Questions 69
What Would You Do? 70
Cases 72
End Notes 76

Chapter 3 *Computer and Internet Crime* 81
Vignette 81
The Reveton Ransomware Attacks 81
IT Security Incidents: A Major Concern 84
Why Computer Incidents Are So Prevalent 84
Types of Exploits 88
Types of Perpetrators 95
Federal Laws for Prosecuting Computer Attacks 99
Implementing Trustworthy Computing 100
Risk Assessment 102
Establishing a Security Policy 104
Educating Employees and Contract Workers 105
Prevention 105
Detection 110
Response 110
Summary 115
Key Terms 116
Self-Assessment Questions 116
Discussion Questions 118
What Would You Do? 118
Cases 120
End Notes 125

Chapter 4 *Privacy* 131
Vignette 131
What Is the National Security Agency (NSA) Up To? 131
Privacy Protection and the Law 133
Information Privacy 135
Privacy Laws, Applications, and Court Rulings 135
Key Privacy and Anonymity Issues 151
Data Breaches 151
Electronic Discovery 153
Consumer Profiling 154

Workplace Monitoring 155
Advanced Surveillance Technology 157
Summary 160
Key Terms 162
Self-Assessment Questions 163
Discussion Questions 164
What Would You Do? 165
Cases 167
End Notes 171

Chapter 5 *Freedom of Expression* 179
Vignette 179
Reputation Changer, Online Reputation Management Company 179
First Amendment Rights 181
Obscene Speech 183
Defamation 183
Freedom of Expression: Key Issues 184
Controlling Access to Information on the Internet 184
Strategic Lawsuit Against Public Participation (SLAPP) 189
Anonymity on the Internet 190
Hate Speech 193
Pornography 194
Summary 199
Key Terms 200
Self-Assessment Questions 201
Discussion Questions 202
What Would You Do? 203
Cases 205
End Notes 209

Chapter 6 *Intellectual Property* 217
Vignette 217
Sinovel Steals Millions in Trade Secrets from American Superconductor 217
What Is Intellectual Property? 220
Copyrights 221
Copyright Term 221
Eligible Works 222
Fair Use Doctrine 222
Software Copyright Protection 223
The Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008 224
General Agreement on Tariffs and Trade (GATT) 224
The WTO and the WTO TRIPS Agreement (1994) 224
The World Intellectual Property Organization (WIPO) Copyright Treaty (1996) 225
The Digital Millennium Copyright Act (1998) 225

Patents 228
Leahy-Smith America Invents Act (2011) 230
Software Patents 230
Cross-Licensing Agreements 231
Trade Secrets 231
Trade Secret Laws 232
Employees and Trade Secrets 233
Key Intellectual Property Issues 234
Plagiarism 234
Reverse Engineering 236
Open Source Code 238
Competitive Intelligence 239
Trademark Infringement 242
Cybersquatting 243
Summary 244
Key Terms 246
Self-Assessment Questions 247
Discussion Questions 248
What Would You Do? 249
Cases 250
End Notes 255

Chapter 7 *Software Development* 261
Vignette 261
Stock Markets Susceptible to Software Glitches 261
Strategies for Engineering Quality Software 264
The Importance of Software Quality 267
Software Product Liability 268
Software Development Process 270
Capability Maturity Model Integration 273
Key Issues in Software Development 275
Development of Safety-Critical Systems 275
Quality Management Standards 279
Summary 282
Key Terms 283
Self-Assessment Questions 284
Discussion Questions 285
What Would You Do? 286
Cases 288
End Notes 292

Chapter 8 *The Impact of Information Technology on Productivity and Quality of Life* 297
Vignette 297
Problems with the E-Rate Program 297
The Impact of IT on the Standard of Living and Worker Productivity 301
IT Investment and Productivity 301
The Digital Divide 306

The Impact of IT on HealthCare Costs 310
Electronic Health Records 310
Use of Mobile and Wireless Technology in the Healthcare Industry 314
Telehealth 315
Medical Information Web Sites for Laypeople 317
Summary 319
Key Terms 320
Self-Assessment Questions 320
Discussion Questions 322
What Would You Do? 322
Cases 324
End Notes 328

Chapter 9 *Social Networking* 335
Vignette 335
Wanelo: Social Shopping Web Site Headed for Success 335
What Is a Social Networking Web Site? 337
Business Applications of Online Social Networking 338
Social Network Advertising 339
The Use of Social Networks in the Hiring Process 342
The Use of Social Media to Improve Customer Service 343
Social Shopping Web Sites 344
Social Networking Ethical Issues 345
Cyberbullying 346
Cyberstalking 347
Encounters with Sexual Predators 348
Uploading of Inappropriate Material 350
Online Virtual Worlds 351
Crime in Virtual Worlds 352
Educational and Business Uses of Virtual Worlds 353
Summary 354
Key Terms 355
Self-Assessment Questions 355
Discussion Questions 356
What Would You Do? 357
Cases 358
End Notes 362

Chapter 10 *Ethics of IT Organizations* 369
Vignette 369
HP Finds Autonomy a Tough Pill to Swallow 369
Key Ethical Issues for Organizations 371
The Need for Nontraditional Workers 372
Contingent Workers 374
Advantages of Using Contingent Workers 375
Disadvantages of Using Contingent Workers 375
Deciding When to Use Contingent Workers 376
H-1B Workers 377

H-1B Application Process 379
Using H-1B Workers Instead of U.S. Workers 380
Potential Exploitation of H-1B Workers 380
Outsourcing 381
Offshore Outsourcing 381
Pros and Cons of Offshore Outsourcing 383
Strategies for Successful Offshore Outsourcing 384
Whistle-Blowing 385
Protection for Whistle-Blowers 386
Whistle-Blowing Protection for Private-Sector Workers 387
Dealing with a Whistle-Blowing Situation 387
Green Computing 390
ICT Industry Code of Conduct 392
Summary 394
Key Terms 395
Self-Assessment Questions 395
Discussion Questions 397
What Would You Do? 398
Cases 401
End Notes 405

Appendix A *A Brief Introduction to Morality* 411
Introduction 411
The Knotty Question of Goodness 412
Relativism: Why "Common Sense" Won't Work 413
Egoism vs. Altruism 414
Deontology, or The Ethics of Logical Consistency and Duty 416
Happy Consequences, or Utilitarianism 418
Promises and Contracts 420
A Return to The Greeks: The Good Life of Virtue 421
Feminism and the Ethics of Care 423
Pluralism 424
Summary 425

Appendix B *Answers to Self-Assessment Questions* 427

Glossary 429

Index 441

PREFACE

We are excited to publish the fifth 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, Fifth 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. 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, Fifth 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, Fifth Edition, has been updated and revised to incorporate the many new developments and ethical issues that have arisen since the last edition. There is new or expanded coverage of the following topics: the increased security risks of bring your own device (BYOD) business policies, the role of the National Security Agency in breaking of codes used to encrypt sensitive communications and for the interception of signals on behalf of the federal government, the ethics of using online reputation management companies, the use of strategic lawsuits against public participation (SLAPP) and anti-SLAPP lawsuits, the theft by China of trade secrets from the United States and Western Europe, and telehealth and telemedicine and their role in the delivery of health care.

All opening vignettes and two-thirds of the end-of-chapter cases are new or extensively updated. Dozens of new real-world examples are presented in each chapter. At least 50 percent of the "Self-Assessment Questions," "Discussion Questions," and "What Would You Do?" exercises are new. Based on reviewer feedback, we have also increased the number of "Discussion Questions" and "What Would You Do?" exercises. Instructors of online courses frequently use these as the basis for discussion forums that allow 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.

ORGANIZATION

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

- Chapter 1, "An Overview of Ethics," provides an introduction to ethics,ethics in business, and the relevance of discussing ethics in IT. The chapter defines the distinction between morals, ethics, and laws. It identifies the most common forms of employee misconduct. The concept of corporate social responsibility is defined and discussed. It presents five reasons why practicing good business ethics is important in business and provides a model for improving corporate ethics. It examines the role of the chief ethics officer and board of directors in establishing a strong organizational ethics program. The chapter also outlines the need for an organizational code of ethics and describes key steps in establishing a sound ethics program. It suggests a model for ethical decision making and also discusses four commonly used philosophical approaches to ethical decision making. The chapter ends with a discussion of the role of ethics in IT.
- Chapter 2, "Ethics for IT Workers and IT Users," begins with a vignette that illustrates major fraud on a real IT project involving the New York City Payroll. This chapter 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 also emphasizes the significance of IT professional organizations and their codes of ethics, and it discusses the roles that certification and licensing can play in legitimizing professional standards. The chapter also points out the difficulties in licensing IT workers. The chapter touches on some ethical issues faced by IT users—including software piracy, inappropriate use of computing resources, and inappropriate sharing of information—and outlines actions that can be taken to support the ethical practices of IT users. The chapter introduces the topic of 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 are in compliance with organizational guidelines and policies, as well as various legal and regulatory practices.
- Chapter 3, "Computer and Internet Crime," 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. Including 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 viruses, worms, Trojan horses, distributed denial-of-service, rootkits, spam,

phishing, spear-phishing, smishing, vishing, and ransom ware. 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 outlines both how to implement trustworthy computing to manage security vulnerabilities and how to respond to specific security incidents to quickly resolve problems and improve ongoing security measures. A process for performing an assessment of an organization's computers and network from both internal and external threats is presented. The chapter discusses the need for a corporate security policy and offers both a process for establishing a security policy and a number of security-related policy templates that can help an organization to quickly develop effective security policies. The roles of the United States Computer Emergency Readiness Team (US-CERT) and the Department of Homeland Security in defending against cyberterrorism are also discussed.

- Chapter 4, "Privacy," begins with a vignette on the National Security Agency and its role in the interception of communications signals on behalf of the federal government. This chapter goes on to explain 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 the Foreign Intelligence Surveillance Act and the USA Patriot Act. The chapter also covers the various regulations affecting the export of personal data from one country to another. 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. The expanding use of electronic discovery, workplace monitoring, camera surveillance, and consumer profiling is discussed. Guidelines and principles for treating consumer data responsibly are offered.
- 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 opens with a discussion of Reputation Changer, an online reputation management company that helps businesses manage potentially damaging information on the Web. It goes on to cover the ways in which the ease and anonymity with which Internet users can communicate can 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 Child 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. Defamation and 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. The opening vignette discusses how a Chinese company stole valuable trade secrets from a U.S. firm and makes the point that the theft of trade secrets by Chinese companies from the U.S. and Western companies represents the "greatest transfer of wealth in history." 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 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 covers several key issues relevant to ethics in IT, including plagiarism, reverse engineering of software, open source code, competitive intelligence gathering, and cybersquatting.
- Chapter 7, "Software Development," provides a thorough discussion of the software development process and the importance of software quality. The opening vignette illustrates how susceptible stock markets are to software glitches. The chapter covers issues 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 analysis, and different approaches to quality assurance testing. The chapter also examines Capability Maturity Model Integration (CMMI), the ISO 9000 family of standards, and the failure mode and effects analysis (FMEA) technique.
- Chapter 8, "The Impact of Information Technology on Productivity and the Quality of Life," examines the effect that IT investment has had on the standard of living and worker productivity around the world. The increase in the use of telework (also known as telecommuting) is discussed, as are the pros and cons of this work arrangement. The chapter also discusses the digital divide and profiles some programs designed to close that gap. The chapter takes a look at the impact of IT on the delivery of health care and healthcare costs. The potential costs and benefits associated with electronic health

records is discussed. Telehealth and telemedicine are defined and their role in the delivery of health care are discussed.

- Chapter 9, "Social Networking," discusses how people use social networks, identifies common business uses of social networks, and examines many of the ethical issues associated with the use of social networks. The opening vignette illustrates how the use of social networks raises many privacy issues. The business applications of social networks are covered including their use in advertising, marketing, the hiring process, and improving employee communications and customer service. Social network ethical issues including cyberbullying, cyberstalking, encounters with sexual predators, and the uploading of inappropriate material are also discussed. The chapter covers virtual life communities and the ethical issues associated with virtual worlds.
- 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. The chapter also discusses the risks, protections, and ethical decisions related to whistleblowing, 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. Finally, the chapter examines a code of conduct for the electronics and information and communications technology (ICT) industries designed to address ethical issues in the areas of worker safety and fairness, environmental responsibility, and business efficiency.
- Appendix A provides an in-depth discussion of how ethics and moral codes developed over time.
- Appendix B provides answers to the end-of-chapter Self-Assessment Questions.

PEDAGOGY

Ethics in Information Technology, Fifth 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.
- **Vignette.** At the beginning of each chapter, a brief real-world example illustrates the issues to be discussed and piques the reader's interest.
- **Questions to Consider.** Carefully crafted focus questions follow the vignette to further highlight topics that are covered in the chapter.

- **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.
- **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.** Each checklist provides a practical and useful list of questions to consider when making a business decision.

End-of-Chapter Material

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

- **Summary.** Each chapter includes a summary of the key issues raised. These items relate 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 included in Appendix B.
- **Discussion Questions.** These more 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, three 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. A set of additional case studies from previous editions will be available at the Cengage Web site to provide the instructor with a wide range of cases from which to select.

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. He has authored over two dozen texts and has taught at the University of Cincinnati, Xavier University (Ohio), Miami University (Ohio), and the College of Mount St. Joseph. He is currently teaching at Strayer University.

Teaching Tools

The following supplemental materials are available when this book is used in a classroom setting. All of these tools are provided to the instructor on a single CD-ROM. You can also find some of these materials on the Cengage Learning Web site at www.cengage.com/sso.

- **Electronic Instructor's Manual.** The Instructor's Manual that accompanies this textbook includes additional instructional material to assist in class preparation, including suggestions for lecture topics. It also includes solutions to all end-of-chapter exercises
- **Cengage Learning Testing Powered by Cognero.** A flexible, online system that allows you to:

- author, edit, and manage test bank content from multiple Cengage Learning solutions
- create multiple test versions in an instant
- deliver tests from your LMS, your classroom or wherever you want

- **PowerPoint Presentations.** This book comes with Microsoft PowerPoint slides for each chapter. The slides 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.
- **Figure Files.** Figure files allow instructors to create their own presentations using figures taken directly from the text.
- **Blackboard and WebCT™ Level 1 Online Content.** If you use Blackboard or WebCT, the test bank for this textbook is available at no cost in a simple, ready-to-use format.

ACKNOWLEDGMENTS

I wish to express my appreciation to a number of people who helped greatly in the creation of this book: Charles McCormick, Jr., Senior Acquisitions Editor, for his belief in and encouragement of this project; Jennifer Feltri-George and Divya Divakaran, Content Product Managers, for guiding the book through the production process; Kate Mason, Senior Content Developer, for overseeing and directing this effort; Mary Pat Shaffer, Development Editor, for her tremendous support, many useful suggestions, and helpful edits; Naomi Friedman, for writing many of the vignettes and cases; and my many students who provided excellent ideas and constructive feedback on the text. I also wish to thank Clancy Martin for writing Appendix A.

In addition, I want to thank an excellent set of reviewers who offered many useful suggestions:

Pat Artz, Bellevue University
Astrid Todd, Guilford Technical Community College
Charles Watkins, Baker College

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

Integrity is doing the right thing, even when nobody is watching.
—Anonymous

VIGNETTE

Cisco Chairman and CEO Advocates Ethical Behavior

Cisco is a U.S.-based multinational corporation that designs, sells, and manufactures networking equipment. The company's operations generated $46 billion in sales and $8 billion in net income for fiscal year 2012.[1] Cisco has been named a "World's Most Ethical Company" honoree by the Ethisphere Institute for five consecutive years (2008–2012).[2] Its Chairman and CEO John Chambers states: "A strong commitment to ethics is critical to our long-term success as a company. The message for each employee is clear: Any success that is not achieved ethically is no success at all. At Cisco, we hold ourselves to the highest ethical standards, and we will not tolerate anything less."[3]

Cisco conducts numerous programs aimed at fulfilling what it sees as its corporate social responsibilities. For instance, the company provides ethics training to its over 70,000 employees, and it prides itself on providing employee benefits that foster a good work-life balance. Cisco employees are also encouraged to donate money and volunteer hours to nonprofit organizations around the world. Cisco manages energy and greenhouse emission generated by its operations. The company

demands the same high standards from its more than 600 supply chain partners in regard to ethics, labor practices, health and safety, and the environment; it communicates its Code of Conduct to suppliers, monitors their compliance, and helps them improve performance. Cisco collaborates with industry groups to raise standards and build sustainability capabilities throughout its supply chain. The company uses its core expertise in networking technology to improve both the delivery and quality of education as well as to improve health care. It also intervenes to help meet critical human needs in times of disaster by providing access to food, potable water, shelter, and other forms of relief. For example, in 2012, Cisco employees pledged $1.25 million and 12,500 volunteer hours to the Global Hunger Relief Program. Both the Cisco Foundation and Cisco Chairman Emeritus John Morgridge match employee donations, thus tripling the potential donation.[4]

Questions to Consider

1. What does it mean for an individual to act in an ethical manner? What does it mean for an organization to act ethically?
2. How should an organization balance its resources between pursuing its primary mission for existence and striving to meet social responsibility goals?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What is ethics, and why is it important to act according to a code of ethics?
2. Why is business ethics becoming increasingly important?
3. What are organizations doing to improve their business ethics?
4. What is corporate social responsibility?
5. Why are organizations interested in fostering corporate social responsibility and good business ethics?
6. What approach can you take to ensure ethical decision making?
7. What trends have increased the risk of using information technology in an unethical manner?

WHAT IS ETHICS?

Every society forms a set of rules that establishes the boundaries of generally accepted behavior. These rules are often expressed in statements about how people should behave, and the individual rules fit together to form the **moral code** by which a society lives. Unfortunately, the different rules often have contradictions, and people are sometimes uncertain about which rule to follow. For instance, if you witness a friend copy someone else's answers while taking an exam, you might be caught in a conflict between loyalty to your friend and the value of telling the truth. Sometimes the rules do not seem to cover new situations, and an individual must determine how to apply existing rules or develop new ones. You may strongly support personal privacy, but do you think an organization should be prohibited from monitoring employees' use of its email and Internet services?

The term **morality** refers to social conventions about right and wrong that are so widely shared that they become the basis for an established consensus. However, individual views of what behavior is moral may vary by age, cultural group, ethnic background, religion, life experiences, education, and gender. 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, and gun control are continuously debated, and people on both sides of these debates feel that their arguments are on solid moral ground.

Definition of Ethics

Ethics is a set of beliefs about right and wrong behavior within a society. Ethical behavior conforms to generally accepted norms—many of which are almost universal. However, although nearly everyone would agree that certain behaviors—such as lying and cheating—are unethical, opinions about what constitutes ethical behavior 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. In 2011, an estimated 43 percent of all personal computer software in circulation worldwide was pirated—at a commercial value of $63 billion (USD).[5] Zimbabwe (92%), Georgia (91%), Bangladesh (90%), Libya (90%), and Moldova (90%) are consistently among the countries with the highest rate of piracy. The United States (19%), Luxembourg (20%), Japan (21%), and New Zealand (22%) are consistently among the countries with the lowest piracy rates.[6]

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 what society considers good or 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.

The Importance of Integrity

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 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?

A person who acts with **integrity** acts in accordance with a personal code of principles. One approach to acting with integrity—one of the cornerstones of ethical behavior—is to extend to all people the same respect and consideration that you expect to receive from others. 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 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

Morals are one's personal beliefs about right and wrong, while the term *ethics* describes standards or codes of behavior expected of an individual by a group (nation, organization, profession) to which an individual belongs. For example, 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.

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). 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.

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, provides advice 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. In the past decade, we have watched 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.[7] Clearly, unethical behavior has led to serious negative consequences that have had a major global impact.

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. For example, numerous U.S. companies have moved operations to developing countries, where employees work in conditions that would not be acceptable in most developed parts of the world.

Second, in today's difficult and uncertain economic climate, organizations are extremely challenged to maintain revenue and profits. Some organizations are sorely tempted to resort to unethical behavior to maintain profits. For example, the chairman of the India-based outsourcing firm Satyam Computer Services admitted he had overstated the company's assets by more than $1 billion. The revelation represented India's largest-ever corporate scandal and caused the government to step in to protect the jobs of the company's 53,000 employees.[8]

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 of unethical decision making can be found in the Enron accounting scandal. In 2000, Enron employed over 22,000 people and had annual revenue of $101 billion. During 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 faulty accounting, 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.[9] 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:

- In 2011, IBM agreed to pay $10 million to settle civil charges arising from a lawsuit filed by the Securities and Exchange Commission (SEC) alleging the firm had violated the Foreign Corrupt Practices Act for bribing government officials in China and South Korea to secure the sale of IBM products. (The act makes it illegal for corporations listed on U.S. stock exchanges to bribe foreign officials.) The bribes allegedly occurred over a decade and included hundreds of thousands of dollars of cash, electronics, and entertainment and travel expenses in exchange for millions of dollars in government contracts.[10]
- The founders of the three largest Internet poker companies were indicted for using fraudulent methods to circumvent U.S. antigambling laws and to obtain billions of dollars from U.S. residents who gambled on their sites.[11]
- The Office of the Comptroller of the Currency (OCC), which oversees large U.S. banks, accused Citibank in 2012 of failing to comply with rules intended to enforce the Bank Secrecy Act. This act is designed to deter and detect money laundering, terrorist financing, and other criminal acts. Citibank neither admitted nor denied the allegations, but the company did agree to provide the OCC with a plan outlining how it would bring its program into compliance.[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 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 can find themselves in the middle of ethical dilemmas, as these examples illustrate:

- A low-level employee of the Technical Services Department of Monroe County, Florida, was entrusted with responsibility for both acquisition and distribution of the county's cell phones. A few months after her retirement, the employee was indicted on charges of stealing 52 county-purchased iPhones and iPads and then selling them to friends and coworkers.[14]
- Army Private First Class Bradley Manning is believed to be responsible for the release of thousands of classified U.S. embassy cables, which caused an incident that became known as *Cablegate*. The incident caused many to seriously question security at the Department of Defense and led to many changes in the handling of intelligence and other classified information at various U.S. intelligence agencies and departments.[15]
- According to CyberSource Corporation (a subsidiary of Visa Inc. that offers e-commerce payment management services), online revenue lost to fraud increased 26 percent from 2010 to 2011 to the amount of $3.4 billion. This represents 1 percent of the $340 billion retail e-commerce sales for the United States and Canada.[16]

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	Percent of surveyed employees observing this behavior
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 Line: Ethics Resource Center, "2011 National Business Ethics Survey: Workplace Ethics in Transition," © 2011, www.ethics.org/nbes/files/FinalNBES-web.pdf.

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 the environment, the community, and the welfare of its employees. Setting CSR goals encourages an organization to achieve higher moral and ethical standards. As highlighted in the opening vignette, Cisco is an example of an organization that has set and achieved a number of CSR goals for itself, and as a result is recognized as a highly ethical company.

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 such issues 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 European Union countries. In many cases, meeting supply chain sustainability goals can also lead to lower costs. For example, since 2001, Intel has invested over $45 million in efforts to reduce its energy costs. As a result of those initiatives, the company has saved on average $23 million per year.[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. For example, many fast-food hamburger outlets (including McDonald's, Wendy's, and Burger King) have expanded their menus to include low-fat offerings in an attempt to meet a CSR goal of providing more healthy choices to their customers, while also trying to capture more market share.[18]

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, some U.S. auto manufacturers have introduced automobiles 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 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 generate an increase in profits from the sale of these electric cars, and senior management at the automakers must consider how long they can continue with this strategy.

Why Fostering Corporate Social Responsibility and Good Business Ethics Is Important

Organizations have at least five good reasons for pursuing CSR goals and for promoting 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. Companies may also issue a formal statement of their company's values, principles, or beliefs. See Figure 1-1 for an example of a statement of values.

Our Values

As a company, and as individuals, we value integrity, honesty, openness, personal excellence, constructive self-criticism, continual self-improvement, and mutual respect. We are committed to our customers and partners and have a passion for technology. We take on big challenges, and pride ourselves on seeing them through. We hold ourselves accountable to our customers, shareholders, partners, and employees by honoring our commitments, providing results, and striving for the highest quality.

FIGURE 1-1 Microsoft's statement of values

Credit: Microsoft Statement of Values, "Our Values," from www.microsoft.com. Reprinted by permission.

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 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. Table 1-2 provides a few examples of some of the CSR activities supported by major IT organizations.

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 best job candidates. On the other hand, companies viewed as harmful to their community may suffer a disadvantage. For example, a corporation that pollutes the environment may find that adverse publicity reduces sales, impedes relationships with some business partners, and attracts unwanted government attention.

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 consistency ensures that employees know what is expected of them and can employ the organization's

TABLE 1-2 Examples of IT organizations' socially responsible activities

Organization	Examples of socially responsible activities
Dell Inc.	Dell partners with nonprofit organizations to develop ways of using technology to help solve pressing problems. Its "Powering the Positive" program initiatives include Children's Cancer Care, Youth Learning, Disaster Relief, and Social Entrepreneurship.[19]
Google	Google recently invested over $250 million in solar and wind power projects.[20]
IBM	IBM employees donated 3.2 million hours of community service in 120 countries in 2011.[21]
Oracle	Oracle supports K-12 and higher education institutions with technology education grants and programs that reach 1.5 million students each year.[22]
SAP, North America	SAP supports several major corporate responsibility initiatives aimed at improving education, matches employee gifts to nonprofit agencies and schools, and encourages and supports employee volunteerism.[23]
Microsoft	Microsoft conducts an annual giving campaign, and its employees have contributed over $1 billion to some 31,000 nonprofit organizations around the world since 1983.[24]

Source Line: Copyright © Cengage Learning. Adapted from multiple sources. See End Notes 19, 20, 21, 22, 23, 24.

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."

The CEO and the general counsel of IT solutions and services provider GTSI Corporation were forced by the Small Business Administration (SBA) to resign, while three other top GTSI executives were suspended, due to allegations that GTSI employees were involved in a scheme with its contracting partners that resulted in the firm receiving money set aside for small businesses. GTSI, which had over 500 employees and revenue over $760 million, was providing services to the Department of Homeland Security in partnership with contractors who qualified as small businesses, but GTSI—as a subcontractor—was actually performing most of the services and being paid most of the fees.[27] In this case, top executives were punished for the acts of several unidentified employees. The company was also suspended by the SBA from receiving new government contracts, and was ultimately acquired by another company after a steep drop in revenue.[28]

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."[29] 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.

In 2012, Google agreed to pay a fine of $22.5 million to end an FTC investigation into allegations that the firm utilized cookies and bypassed privacy settings to track the online habits of people using Apple's Safari browser. The amount of the fine, while the largest in FTC history, represented less than one day's worth of Google's profits. However, some IT industry analysts believe that the bad publicity associated with the incident is much more impactful than the fine in bringing about change at Google and in keeping it from violating FTC rules in the future.[30]

Improving Corporate 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 1-2.[31]

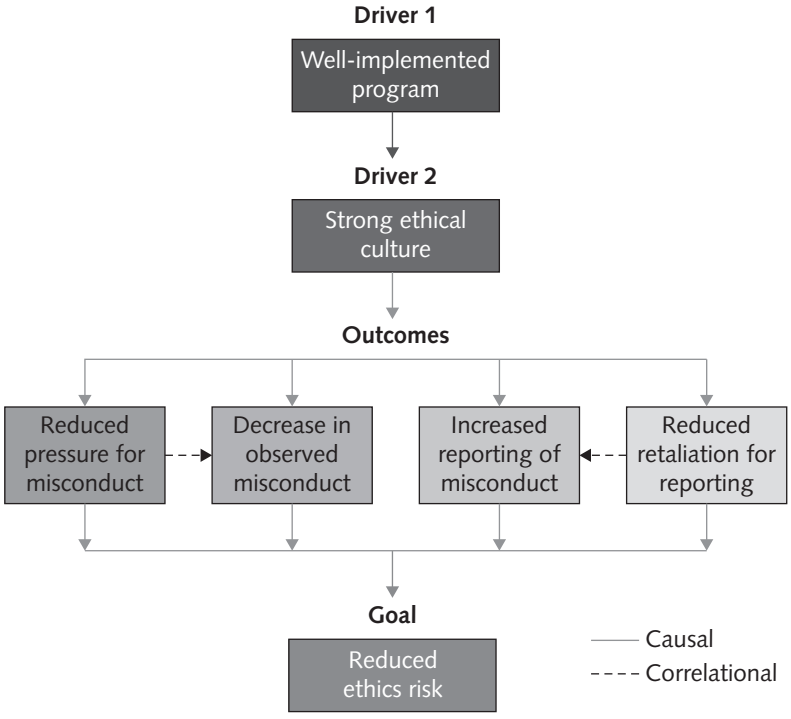


FIGURE 1-2 Reducing ethics risk

Credit: Courtesy Ethics Resource Center, "2011 National Business Ethics Survey: Workplace Ethics in Transition"

The ERC has defined the following characteristics of a successful ethics program:

- Employees are willing to seek advice about ethics 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.

In its 2011 National Business Ethics Survey, based on responses from over 3,000 individuals, the ERC found evidence of some improvement in ethics in the workplace as summarized in Table 1-3.[32] These figures show that fewer employees witnessed misconduct on the job, but when they did, they were more willing to report it. The findings also show that there are more employees who feel pressure to commit an unethical act, as well as more employees who feel their organization has a weak ethics culture.

TABLE 1-3 Conclusions from the National Business Ethics Survey

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

Source Line: Ethics Resource Center, "2011 National Business Ethics Survey, Workplace Ethics in Transition," www.ethics.org/news/new-research-2011-national-business-ethics-survey.

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.

Appointing 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 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 the 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. 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—who has been the director of compliance at Microsoft for over a decade—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 that the highest level of corporate authority wishes to have
- 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.

Ethical Standards Set by Board of Directors

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. Failure of the board to set an example of high-level ethical behavior or to intervene to stop unethical behavior can result in serious consequences as illustrated by the News Corporation scandal.

News Corporation is a media conglomerate founded by Rupert Murdoch—with recent annual revenue over $30 billion generated by its cable networks (including Fox News Channel), film and television production subsidiaries, and publishing units. In 2009, it came to light that News Corporation's British subsidiary, News International Ltd., publisher of the highly popular Sunday tabloid paper, *News of the World*, used telephone hacking and bribes to police to obtain stories about celebrities, sports figures, politicians, and ordinary citizens.[37] It was alleged that the practice was well known to senior executives within the company. Based on strong negative public reaction, News Corporation stopped publication of the *News of the World* tabloid, and the British government blocked a major deal in which News Corporation was to fully acquire the highly successful British broadcasting company BSkyB. These actions resulted in a $3 billion drop in the stock value of News Corporation. In addition, the scandal led to the arrest of over 60 former and current journalists, and many high-level executives resigned from the firm. In a lawsuit filed in March 2011, shareholders claimed lack of board oversight for failing to react to warning signals that should have alerted them to the telephone hacking.[38]

Establishing 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.

The **Sarbanes–Oxley Act of 2002** was passed in response to public outrage over several major accounting scandals, including those at Enron, WorldCom, Tyco, Adelphia, Global Crossing, and Qwest—plus numerous restatements of financial reports by other companies, which clearly demonstrated a lack of oversight within corporate America. The goal of the bill was to renew investors' trust in corporate executives and their firms' financial reports. The act led to significant reforms in the content and preparation of disclosure documents by public companies. However, the Lehman Brothers accounting fiasco and resulting collapse as well as other similar examples raise questions about the effectiveness of Sarbanes–Oxley in preventing accounting scandals.[39]

Section 404 of the act states that annual reports must contain a statement signed by the CEO and CFO attesting that the information contained in all of the firm's SEC filings is accurate. The company must also submit to an audit to prove that it has controls in place to ensure accurate information. The penalties for false attestation can include up to 20 years in prison and significant monetary fines for senior executives. Section 406 of

the act also requires public companies to disclose whether they have a code of ethics and to disclose any waiver of the code for certain members of senior management. The SEC also approved significant reforms by the NYSE and NASDAQ that, among other things, require companies listed with those exchanges to have codes of ethics that apply to all employees, senior management, and directors.

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 U.S. publicly held companies, using a statistical analysis of corporate ethical performance in several categories. (For 2012, the categories were environment, climate change, human rights, employee relations, governance, philanthropy, and financial.) 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 third in 2012.[40] 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 shown in Figure 1-3. A more detailed version is spelled out in a 22-page document (Intel Code of Conduct, January 2012, found at *www.intel.com/content/www/us/en/policy/policy-code-conduct-corporate-information.html*), which offers employees guidelines designed to deter wrongdoing,

INTEL CODE OF CONDUCT
JANUARY 2012

Code of Conduct

Since the company began, uncompromising integrity and professionalism have been the cornerstones of Intel's business. In all that we do, Intel supports and upholds a set of core values and principles. Our future growth depends on each of us understanding these values and principles and continuously demonstrating the uncompromising integrity that is the foundation of our company.

The Code of Conduct sets the standard for how we work together to develop and deliver product, how we protect the value of Intel and its subsidiaries (collectively known as 'Intel'), and how we work with customers, suppliers and others. All of us at Intel must abide by the Code when conducting Intel-related business.

The Code affirms our five principles of conduct:

- Conduct Business with Honesty and Integrity
- Follow the Letter and Spirit of the Law
- Treat Each Other Fairly
- Act in the Best Interests of Intel and Avoid Conflicts of Interest
- Protect the Company's Assets and Reputation

FIGURE 1-3 Intel's Code of Conduct

Credit: Intel's Code of Conduct. © Intel Corporation. Reprinted by permission.

promote honest and ethical conduct, and comply with applicable laws and regulations. Intel's Code of Conduct also expresses its policies regarding the environment, health and safety, intellectual property, diversity, nondiscrimination, supplier expectations, privacy, and business continuity.

Conducting 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. For example, each year Intel prepares its "Corporate Responsibility Report," which summarizes the firm's progress toward meeting its ethical and CSR goals. In 2011, Intel focused on goals in three primary areas: (1) the environment—with targets set for global-warming emissions, energy consumption, water use, chemical and solid waste reduction, and product energy efficiency; (2) corporate governance—with goals to improve transparency and strengthen ethics and compliance reporting; and (3) social—with goals to improve the organizational health of the company as measured by its own Organizational Health Survey, to expand the number of supplier audits, and to increase the number of community education programs.[41]

Requiring 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 top to bottom. Organizations can do this by showing 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 2011 National Business Ethics Survey, the Ethics Resource Center reported that 56 percent of all complaints are reported to an employee's direct supervisor.[42] Because these supervisors are essentially the eyes and ears of the company, they "need adequate resources, support, and training to address the stress created by and

the additional misconduct related to the implementation of company tactics" according to the ERC.[43]

Motorola, designer of wireless network equipment, cell phones, and smartphones, is committed to a strong corporate ethics training program to ensure that its employees conduct its business with integrity. The focus of the training is to clarify corporate values and policies and to encourage employees to report ethical concerns via numerous reporting channels. Motorola investigates all allegations of ethical misconduct, and it will take appropriate disciplinary actions if a claim is proven—up to and including dismissal of all involved employees. All salaried employees must complete an online introduction to the ethics program every three years. All managers in newly acquired businesses or high-risk locations must take further classroom ethics training. Motorola operates a 24-hour toll-free service for reporting any suspected ethical concerns. In 2011, the firm introduced a Code of Business Conduct in 10 languages and updated its suite of ethics training courses to include new anticorruption and antibribery training.[44]

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.

Including 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.

Creating 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.

Here are a few 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."

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 Web site 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 provides a manager's checklist for establishing an ethical workplace. The preferred answer to each question is *yes*.

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?		

Source Line: Course Technology/Cengage Learning.

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 1-4.

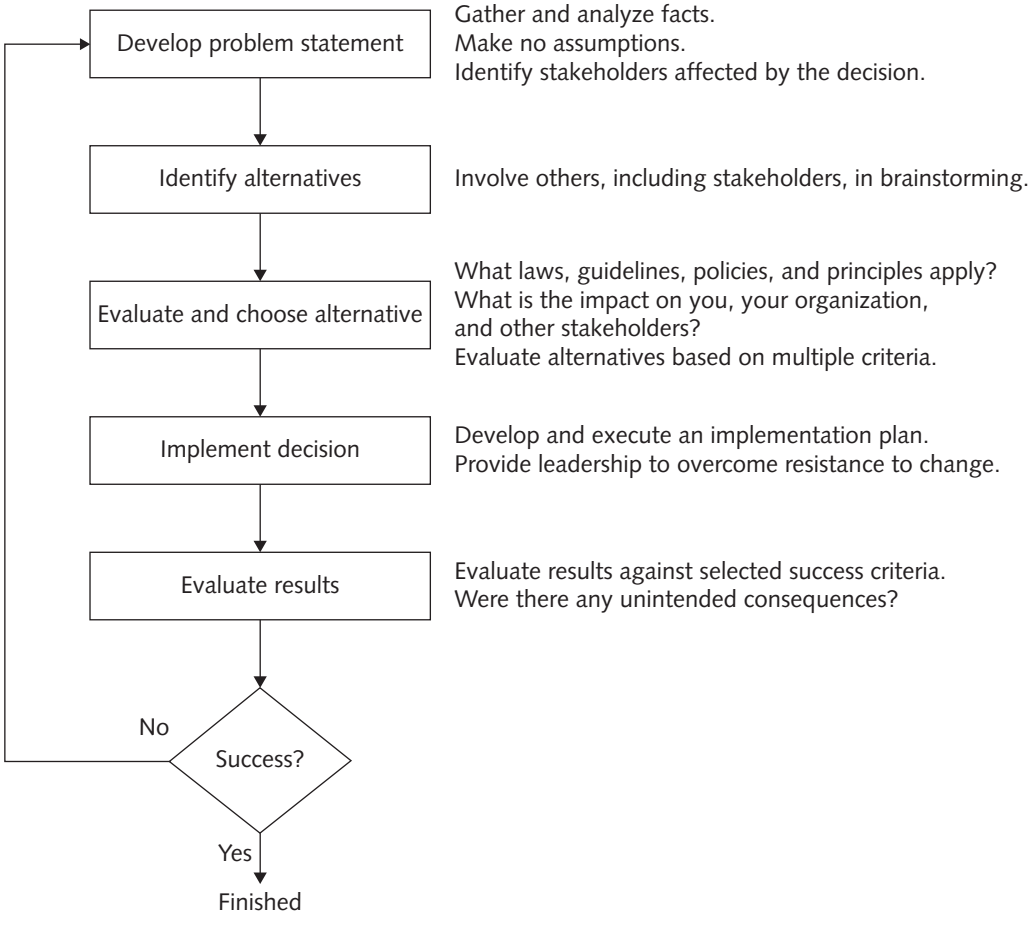


FIGURE 1-4 Decision-making process

Source Line: Course Technology/Cengage Learning.

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 a 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? 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. Obviously, if the problem is stated incorrectly, the decision will not solve the problem.

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. Simple situations can sometimes turn into complex controversies because no one takes the time to gather the facts. For example, you might see your boss receive what appears to be an employment application from a job applicant and then throw the application into the trash after the applicant leaves. This would violate your organization's policy to treat each applicant with respect and to maintain a record of all applications for one year. You could report your boss for failure to follow the policy, or you could take a moment to speak directly to your boss. You might be pleasantly surprised to find out that the situation was not as it appeared. Perhaps the "applicant" was actually a salesperson promoting a product for which your company had no use, and the "application" was marketing literature.

Part of developing a good problem statement involves identifying the stakeholders and their positions on the issue. Stakeholders often include others beyond those directly involved in an issue. Identifying the stakeholders helps you understand the impact of your decision and could help you make a better decision. Unfortunately, it may also cause you to lose sleep from wondering how you might affect the lives of others. However, by involving stakeholders in the decision, you can work to gain their support for the recommended course of action. What is at stake for each stakeholder? What does each stakeholder value, and what outcome does each stakeholder want? Do some stakeholders have a greater stake because they have special needs or because the organization has special obligations to them? To what degree should they be involved in the decision?

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.)
- Poor problem statement: We have a problem with finished product inventory. (This is not specific enough.)

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.

Evaluate and Choose an Alternative

Once a set of alternatives has been identified, the group must evaluate them based on numerous criteria, such as effectiveness at 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 personal principles apply?

Also 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?

The alternative selected should be ethically and legally defensible; 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.

Philosophers have developed many approaches to aid in ethical decision making. Four of the most common approaches, which are summarized in Table 1-5 and discussed in the following sections, provide a framework for decision makers to reflect on the acceptability of their actions and evaluate their moral judgments. People must find the appropriate balance among all applicable laws, corporate principles, and moral guidelines to help them make decisions. (See Appendix A for a more in-depth discussion of ethics and moral codes.)

TABLE 1-5 Summary of four common approaches to ethical decision making

Approach to dealing with ethical issues	Principle
Virtue ethics approach	The ethical choice best reflects moral virtues in yourself and your community.
Utilitarian approach	The ethical choice produces the greatest excess of benefits over harm.
Fairness approach	The ethical choice treats everyone the same and shows no favoritism or discrimination.
Common good approach	The ethical choice advances the common good.

Source Line: Course Technology/Cengage Learning.

Virtue Ethics Approach

The **virtue ethics approach** to decision making focuses on how you should behave and think about relationships if you are concerned with your daily life in a community. It does not define a formula for ethical decision making, but suggests that when faced with a complex ethical dilemma, people do either what they are most comfortable doing or what they think a person they admire would do. The assumption is that people are guided by their virtues to reach the "right" decision. A proponent of virtue ethics believes that a disposition to do the right thing is more effective than following a set of principles and rules, and that people should perform moral acts out of habit, not introspection.

Virtue ethics can be applied to the business world by equating the virtues of a good businessperson with those of a good person. However, businesspeople face situations that are peculiar to a business setting, so they may need to tailor their ethics accordingly. For example, honesty and openness when dealing with others are generally considered virtues; however, a corporate purchasing manager who is negotiating a multimillion dollar deal might need to be vague in discussions with potential suppliers.

A problem with the virtue ethics approach is that it doesn't provide much of a guide for action. The definition of *virtue* cannot be worked out objectively; it depends on the circumstances—you work it out as you go. For example, bravery is a great virtue in many circumstances, but in others it may be foolish. The right thing to do in a situation also depends on which culture you're in and what the cultural norm dictates.

Utilitarian Approach

The **utilitarian approach** to ethical decision making states that you should choose the action or policy that has the best overall consequences for all people who are directly or indirectly affected. The goal is to find the single greatest good by balancing the interests of all affected parties.

Utilitarianism fits easily with the concept of value in economics and the use of cost-benefit analysis in business. Business managers, legislators, and scientists weigh the benefits and harm of policies when deciding whether to invest resources in building a new plant in a foreign country, to enact a new law, or to approve a new prescription drug.

A complication of this approach is that measuring and comparing the values of certain benefits and costs is often difficult, if not impossible. How do you assign a value to human life or to a pristine wildlife environment? It can also be difficult to predict the full benefits and harm that result from a decision.

Fairness Approach

The **fairness approach** focuses on how fairly actions and policies distribute benefits and burdens among people affected by the decision. The guiding principle of this approach is to treat all people the same. However, decisions made with this approach can be influenced by personal bias, without the decision makers even being aware of their bias. If the intended goal of an action or a policy is to provide benefits to a target group, other affected groups may consider the decision unfair.

Common Good Approach

The **common good approach** to decision making is based on a vision of society as a community whose members work together to achieve a common set of values and goals. Decisions and policies that use this approach attempt to implement social systems, institutions, and environments that everyone depends on and that benefit all people. Examples include an effective education system, a safe and efficient transportation system, and accessible and affordable health care.

As with the other approaches to ethical decision making, the common good approach has potential complications. People clearly have different ideas about what constitutes the common good, which makes consensus difficult. In addition, maintaining the common good often requires some groups to bear greater costs than others—for instance, homeowners pay property taxes to support public schools, but apartment dwellers do not.

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 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.

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 develop a problem statement step, refine the problem statement as necessary, and work through the process again.

ETHICS IN INFORMATION TECHNOLOGY

The growth of the Internet, the ability to capture and store vast amounts of personal data, and 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:

- 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 (spam) as an extremely low-cost marketing approach.
- Hackers break into databases of financial and retail institutions to steal customer information, 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.
- Web sites 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. Unlike most conventional tools, IT has a profound effect on society. IT professionals and end users need to recognize this fact when they 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 in the business world, important decisions are too often left to the technical experts. General business managers must assume greater responsibility for these decisions, but to do so they must be able to make broad-minded, objective decisions based on technical savvy, business know-how, and a sense of ethics. 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.

Summary

- Even within the same society, people can have strong disagreements over important moral issues.
- 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.
- Each organization must decide if corporate social responsibility (CSR) is a priority for it 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.
- Organizations have five good reasons for 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.
- An organization with a successful ethics program is one in which employees are willing to seek advice about ethical issues that arise, employees feel prepared to handle situations that could lead to misconduct, employees are rewarded for ethical behavior, employees are not rewarded for success gained through questionable means, and employees feel positively about their company.
- The corporate ethics officer (or corporate compliance officer) ensures that ethical procedures are put into place and are consistently adhered to throughout the organization, creates and maintains the ethics culture, and serves as a key resource on issues relating to corporate principles and ethics.
- Managers' behavior and expectations can strongly influence employees' ethical behavior.
- Most of us have developed a simple decision-making model that includes these steps: (1) Develop a problem statement, (2) identify alternatives, (3) evaluate and choose an alternative, (4) implement the decision, and (5) evaluate 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, your stakeholders, your customers and suppliers, and the environment.
- Philosophers have developed many approaches to ethical decision making. Four common philosophies are the virtue ethics approach, the utilitarian approach, the fairness approach, and the common good approach.

Key Terms

Bathsheba syndrome
code of ethics
common good approach
corporate compliance officer
corporate ethics officer
corporate social responsibility (CSR)
ethics
fairness approach
integrity
law
moral code
morality
morals
problem statement
Sarbanes–Oxley Act of 2002
social audit
software piracy
supply chain sustainability
stakeholder
utilitarian approach
vice
virtue
virtue ethics approach

Self-Assessment Questions

The answers to the Self-Assessment Questions can be found in Appendix B.

Choose the word(s) that best complete the following sentences.

1. The term _____ refers to social conventions about right and wrong that are so widely shared that they become the basis for an established consensus.
2. _____ is a set of beliefs about right and wrong behavior within a society.
3. _____ are habits of acceptable behavior.
4. A person who acts with integrity acts in accordance with a personal _____.
5. _____ are one's personal beliefs about right and wrong.
6. _____ is the concept that an organization should act ethically by taking responsibility for the impact of its actions on the environment, the community, and the welfare of its employees.
7. _____ 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.
8. The public _____ of an organization 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.
9. The corporate ethics officer provides the organization with _____ and _____ in the area of business conduct.
10. _____ is a system of rules that tells us what we can and cannot do.
11. _____ requires public companies to disclose whether they have codes of ethics and disclose any waiver to their code of ethics for certain members of senior management.
12. The goal of the Sarbanes–Oxley Act was to _____.

13. _____ highlights an organization's key ethical issues and identifies the overarching values and principles that are important to the organization and its decision-making process.
14. A(n) _____ enables an organization to review how well it is meeting its ethical and social responsibility goals, and communicate new goals for the upcoming year.
15. _____ makes employees more aware of a company's code of ethics and how to apply it, as well as demonstrates that the company intends to operate in an ethical manner.
16. The most important part of the decision-making process is _____.
17. The _____ approach to ethical decision making is based on a vision of society as a community whose members work together to achieve a common set of values and goals.
18. _____ is a clear, concise description of the issue that needs to be addressed.

Discussion Questions

1. There are many ethical issues about which people hold very strong opinions—abortion, gun control, and the death penalty, to name a few. If you were a team member on a project with someone whom you knew held an opinion different from yours on one of these issues, how would it affect your ability to work effectively with this person?
2. Identify two important life experiences that helped you define your own personal code of ethics.
3. Create a list of 5 to 10 guidelines for ensuring a successful brainstorming session to identify potential solutions to a problem.
4. Do you believe an organization should be able to escape criminal liability for the acts of its employees if it has acted as a responsible corporate citizen, making strong efforts to prevent and detect misconduct in the workplace? Why or why not?
5. The Ethics Resource Center identified five characteristics of a successful ethics program. Suggest a sixth characteristic, and defend your choice.
6. Identify three CSR goals that would be appropriate for a large, multinational IT consulting firm. Create three such goals for a small, local IT consulting firm.
7. It is a common practice for managers to hold people accountable to meet "stretch" goals, quotas, and budgets. How can this be done in a way that does not encourage unethical behavior on the part of employees?
8. Describe a hypothetical situation in which the action you would take is not legal, but it is ethical. Describe a hypothetical situation where the action you would take is legal, but not ethical.
9. 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.
10. This chapter discusses four approaches to dealing with moral issues. Which approach is closest to your way of analyzing moral issues? Now that you are aware of different approaches, do you think you might modify your approach to include other perspectives? Explain why or why not.

11. It can be difficult for a large organization to act ethically consistently across all facets of its business. Identify a recent example of a usually ethical company acting in an unethical manner.
12. Should software piracy within the boundaries of third-world countries be tolerated to allow these countries an opportunity to move more quickly into the information age? Why or why not?
13. Without revealing the name of your employer, comment on the efforts of your employer to promote a work environment in which employees are encouraged to act ethically.
14. Do you think that ethics training can really be effective in changing the behavior of employees? 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. You are a recent new hire at your company and have been given the responsibility for soliciting the employees in your 10-person department for the company's annual drive to support United Way (a national nonprofit organization that works with a coalition of volunteers, contributors, and local charities to help people in their own communities). Your company sets "giving goals" based on each employee's annual salary. You have completed your initial solicitation of your coworkers, and several of them declined to contribute, while others have pledged amounts well under their "giving goal." As a result, your department is a few thousand dollars short of its goal. You have a meeting this afternoon with the senior vice president responsible for the company's United Way program. You are concerned that you may be pressured to resolicit and encourage under contributors to pledge more. Do you think that this is a fair request? How would you respond if such pressure is applied to you?
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 15 managers and 10 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. How would you proceed?
3. You are the customer support manager for a small software manufacturer. The newest addition to your 10-person team is Sofia, a recent college graduate. She is a little overwhelmed by the volume of calls, but is learning quickly and doing her best to keep up. Today, as you performed your monthly review of employee email, you were surprised to see that Sofia has received several messages from employment agencies. One message says, "Sofia, I'm sorry you don't like your new job. We have lots of opportunities that I think would much better match your interests. Please call me, and let's talk further." 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. You know that Sofia did not intend for you to see the email, but you can't ignore what you saw. Should you confront Sofia and demand to know her intentions? Should you avoid any confrontation and simply begin seeking her replacement? Could you be misinterpreting the email? What should you do?

4. 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?
5. While mingling with neighbors at a party, you mention that you are responsible for evaluating bids for a large computer software contract. A few days later, you receive a lunch invitation from one of your neighbors who also attended the party. Over appetizers, the conversation turns to the contract you are managing. Your neighbor seems remarkably well informed about the bidding process and likely bidders. You volunteer information about the potential value of the contract and briefly outline the criteria your firm will use to select the winner. At the end of the lunch, your neighbor surprises you by revealing that he is a consultant for several companies in the computer software market. Later that day, your mind is racing. Did you reveal information that could provide a supplier with a competitive advantage in the bidding process? What are the potential business risks and ethical issues in this situation? Should you report the conversation to someone? If so, whom should you talk to, and what would you say?
6. 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 Web sites; 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 and that your responsibilities were greater than they actually were. What would you do?
7. You have just completed a grueling 10-day business trip calling on two dozen accounts up and down the West Coast. 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. IBM–A Front-Runner in Sustainability

During the 1970s, IBM produced mainframe computers, adding machines, typewriters, and telephone routing systems—much of the advanced information technology of the time. The company was the one of the largest corporations in the world and ranked seventh in the 1976 Fortune 500 list of largest U.S. corporations.[45] However, IBM's component manufacturing processes produced large amounts of benzene-based materials that are carcinogenic. In an effort to take the lead in corporate responsibility, IBM established one of the first environmental programs of its kind in 1971.

The company implemented a three-pronged program that attempted to track waste from creation to disposal, to reduce IBM's reliance on toxic chemicals, and to reduce the amount of toxic waste released during the manufacturing process. IBM incrementally reduced toxic waste by 220,500 tons from 1987 to 2011, a dramatic achievement. IBM has been able to accomplish this, in part, by recycling 44 percent of the hazardous chemicals used in its manufacturing processes. The company has also changed manufacturing processes to eliminate or reduce the use of hazardous materials.[46]

Throughout the late twentieth century, IBM was an industry leader in its efforts to address a variety of environmental issues. For example, in the 1980s, scientists noticed a hole in the ozone layer of the stratosphere over Antarctica that protects the earth from harmful ultraviolet radiation. In response, IBM worked to reduce its use of ozone-depleting chemicals, such as chlorofluorocarbons, and in 1989, IBM led the IT world in its reduction of such chemicals.

Today, the company has expanded its initiative beyond toxic waste management. Its programs now seek to reduce energy use, conserve water resources, create energy efficient products, spearhead safety in the use of nanotechnology, and combat climate change. IBM has also focused on the use of environmentally preferable substances and materials, and it continues to work to reduce or eliminate its reliance on heavy metals and carcinogens. The company reduced greenhouse gas emissions in 2011 by 3.2 percent.[47]

IBM works with the International Organization for Standardization (ISO) to create international standards for toxic and nontoxic waste reduction, water purification, efficient energy utilization, and waste emissions. In many cases, IBM helped ISO to develop a specific standard and then became the first company to demonstrate compliance with that standard. In 2011, IBM became the first corporation to meet ISO standards on energy management systems. The practice of meeting sustainability standards helps IBM maintain market share because the European Union, the United States, and other countries often give preference in awarding contracts to companies that have ISO certification. Maintaining market share is more challenging for IBM than it was in the company's early days because many companies now compete with IBM. Samsung, Hewlett-Packard, Nippon Telephone and Telegraph, Apple, Dell, and other companies have crowded the market. By 2012, IBM had dropped to 19 on the Fortune 500 list.[48]

Leveraging ISO certification helps IBM in its efforts to maintain market share and increase its revenue. In fact, the company has found that corporate responsibility has given it a better bottom line. During 2011, IBM spent $114.5 million on its environmental initiatives. During the same period, savings from environmental policies totaled at least $139 million.[49] Company reports indicate that in each of the past 20 years, the savings from its sustainability and environmental stewardship programs have exceeded the costs.

IBM also has an expansive community and corporate citizenship program. For instance, the company has a program to match employees with community service needs. Over 220,000 IBM employees and retirees have participated in this volunteer program in areas such as education, economic development, health care, disaster relief, and environmental programs. IBM also provides employees to serve as teachers for inner city schools throughout the world. The company continues to pay its employees as they work in the schools. Finally, the company utilizes its technology in cities worldwide to help struggling governments find solutions to problems with traffic, emergency services, and infrastructure.[50]

As a company, IBM has set up a steering committee and working group to draft goals and implement CSR strategies. IBM built an electronic meeting platform called Jams, which facilitates online brainstorming and engages a wide range of stakeholders. Since 2001, this platform has not only facilitated the collaboration of 300,000 IBM employees from all over the world, but it has also brought thousands of people from government agencies, nonprofits, corporations, and educational institutions together to identify and address the world's greatest challenges.[51] IBM has been a front-runner in environmental stewardship, and the IT giant has set challenging goals for itself in other areas of CSR.

Discussion Questions

1. Present three strong arguments that IBM might have used to justify the start of its sustainability programs in the 1970s.
2. What major goals has IBM achieved in environmental stewardship?
3. How might IBM leverage its leadership in sustainability to maintain its competitiveness in the IT market?

2. Ethical and Business Setbacks for Nokia

On the morning of September 5, 2012, Nokia staged a press conference in New York City to announce the official launch of its new Windows 8 smartphones, the Lumia 920 and 820. The event focused heavily on the phone's PureView camera technology. Videos played at the press conference and online emphasized the phone's stabilizing technology. One advertisement in particular extolled the steadiness of the smartphone's camera with a video showing a woman bicycling by a riverbank in Helsinki, supposedly shot on a Lumia 920 by a young man bicycling beside the woman. However, the online tech magazine *The Verge* decided to take a closer look at the video, and while examining it, a researcher for the magazine noticed a reflection in a window of a trailer behind the woman on the bike. The reflection showed a young man not on a bicycle, but rather in a van—holding a large camera.[52] Further investigation revealed that the shot was taken by a steadicam, a professional motion picture camera, held by a cameraman in the van.[53] By 4:30 p.m. Eastern time, the word was out. And by 8:00 p.m. the same day, Nokia had updated the video with a disclaimer and issued a formal apology.[54]

Five days after the Lumia advertisement fiasco, Nokia announced that it would conduct an ethics review of the incident. "What we understand to date is that it was nobody's intention to mislead, but there was poor judgment in the decision not to use a disclaimer," Nokia spokesperson Susan Sheehan said. She refused to identify the company responsible for producing the advertisement and stated that Nokia would conduct its investigation "quickly, fairly and

privately."[55] The company quickly concluded its investigation, but has not revealed the results of its investigation, other than to acknowledge that "poor judgment" was used.[56] Nor has Nokia not made public any ethics initiative or punitive measures taken as a result of the false advertisement.

Nokia is one of the world's largest mobile phone manufacturers. It has a 120-year history of worker- and community-centered operations, and a sterling reputation for environmental consciousness. Its corporate manifesto, "The Nokia Way," emphasizes people-centered decision making in a network of equals.[57] The camera fiasco, however, was the latest in a string of ethical and business setbacks that have set the giant corporation reeling.

Nokia announced in 2007 that it was moving production from its facility in Bochum, Germany, to the relatively low-wage environment of Romania.[58] A consumer backlash ensued. The company was eventually required to pay 60 million Euros ($93 million) back to the German state for subsidies paid to the company for locating its facilities in Germany. In addition, a boycott was organized by German trade unions, and several cabinet ministers publicly changed to other brands of cell phones.[59] Nokia saw its share of the German smartphone market drop from 70 percent to 50 percent between the factory closure announcement and the end of 2009. Ironically, Nokia's 2011 decision to close the Romanian facility and move manufacturing to Asia met with similar reactions in Romania.[60]

In 2008, Nokia Siemens Networks, a joint venture between Nokia and Siemens AG, reportedly provided Iran's monopoly telecom company with technology that allowed it to intercept the Internet communications of its citizens to an unprecedented degree.[61] The technology enables the Iranian government to monitor voice calls, text messaging, instant messages, and Web traffic.[62] Nokia officials insisted that the system constituted "a standard architecture that the world's governments use for lawful intercept" and added that the company had refused to sell the technology to the governments of Burma and China.[63] However, in June 2009, the emerging pro-democracy movement in Iran organized a boycott of Nokia devices and messaging services.[64] Finally, on June 2, 2010, Nokia Siemens Networks held a press conference to apologize for the role its technology played in the brutal crackdown on Iranian demonstrators the year before.[65] In late 2011, Nokia-Siemens Networks announced that it would begin to reduce its business commitments in Iran and would no longer take on any new business with Iranian customers.[66]

In 2009, the company strongly supported a law in its native Finland allowing for corporations to monitor the electronic correspondence of its workers. While the protection of trade secrets is a legitimate corporate goal, and similar activities are allowed in many European Union countries, Finnish culture is strongly in favor of privacy and the right to confidentiality.[67] The campaign did little to reassure workers that the Nokia commitment to trust and open decision making was going to continue.

The last several years have also been a time of unprecedented financial upheaval for Nokia. Since 2009, Nokia has lost over a third of its revenues, downsized its workforce by about 25 percent, and seen its market capitalization drop by over $100 billion.[68] While the Lumia line of smartphones continues to be the market leader in Europe, Nokia's share of the U.S. market has dropped to less than one percent.[69] The public's response to Nokia's poor ethical decisions has cost the company heavily. The question remains whether Nokia will learn from its current troubles and adapt quickly enough to satisfy its customers, shareholders, and other stakeholders.

Discussion Questions

1. Were Nokia's leaders acting unethically when they moved their facilities from Germany to Romania and from Romania to Asia, or was this a legitimate business decision to reduce costs and improve profits? How does this decision compare with Nokia's actions in Iran?
2. Why did Nokia's customer base in Europe and Iran react to the company's decisions by withdrawing patronage? Do customers always respond to unethical decisions in this way?
3. How difficult is it to ensure ethical decision making in a business that is organized as a "network of equals"? How does this impact accountability? Does this explain why Nokia kept the investigation secret?

3. Is There a Place for Ethics in IT?

On March 15, 2005, Michael Schrage published an article in *CIO* magazine entitled "Ethics, Schmethics," which stirred up a great deal of controversy in the IT community. In the article, Schrage proposed that CIOs (chief information officers) "should stop trying to do the 'right thing' when implementing IT and focus instead on getting their implementations right." Schrage argued that *ethics* had become a buzzword, just like *quality* in the 1980s; he asserted that the demand for ethical behavior interferes with business efficiency.

In the article, Schrage provided a few scenarios to back up his opinion. In one such example, a company is developing a customer relationship management (CRM) system, and the staff is working very hard to meet the deadline. The company plans to outsource the maintenance and support of the CRM system once it is developed, meaning that there is a good chance that two-thirds of the IT staff will be laid off. Would you disclose this information? Schrage answered, "I don't think so."

In another scenario, Schrage asked readers if they would consider deliberately withholding important information from their boss if they knew that its disclosure would provoke his or her immediate counterproductive intervention in an important project. Schrage said he would withhold it. Business involves competing values, he argued, and trade-offs must be made to keep business operations from becoming paralyzed.[70]

Schrage was hit with a barrage of responses accusing him of being dishonorable, shortsighted, and lazy. Other feedback provided new perspectives on his scenarios that Schrage had not considered in his article. For example, an IT manager at Boise State University argued that doing the right thing is good for business. Not disclosing layoffs, she argued, is a trick that only works once. Remaining employees will no longer trust the company and may pursue jobs where they can feel more secure. New job applicants will think twice before joining a company with a reputation for exploiting employees. Other readers responded to that scenario by suggesting that the company could try to maintain loyalty by offering incentives for those who stayed or by providing job-placement services to departing employees.

Addressing the second scenario, another reader, Dewey, suggested that not giving the boss important information could backfire on the employee: "What if your boss finds out the truth? What if you were wrong and the boss could have helped? Once your boss knows that you lied once, will he believe you the next time?"

Another reader had actually worked under an unproductive, reactive, meddling boss. Based on his experience, he suggested speaking to the boss about the problem at an appropriate time and place. In addition, the reader explained that as situations arose that required him to convey

important information that might elicit interference, he developed action plans and made firm presentations to his boss. The boss, the reader assured Schrage, will adapt.

Some readers argued that CIOs must consider the company's long-term needs rather than just the current needs of a specific project. Others argued that engaging in unethical behavior, even for the best of purposes, crosses a line that eventually leads to more serious transgressions. Some readers suspected that Schrage had published the article to provoke outrage. Another reader agreed with Schrage, arguing that ethics has to "take a back seat to budgets and schedules" in a large organization. This reader explained, "At the end of the day, IT is business."

Discussion Questions

1. Discuss how a CIO might handle Schrage's scenarios using the suggested process for ethical decision making presented in this chapter.
2. Discuss the possible short-term losses and long-term gains in implementing ethical solutions for each of Schrage's scenarios.
3. Must businesses choose between good ethics and financial benefits? Explain your answer using Schrage's scenarios as examples.
4. What do you think Schrage means when he says that CIOs "should stop trying to do the 'right thing' when implementing IT and focus instead on getting their implementations right"? Do you agree?

End Notes

[1] Cisco, "Press Release: Cisco Reports Fourth Quarter and Fiscal Year 2012 Earnings," August 15, 2012, http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=985839.

[2] Ethisphere Institute, "2012 World's Most Ethical Companies," http://ethisphere.com/wme (accessed November 25, 2012).

[3] Cisco, "Ethics@Cisco: Connecting with Our Values," www.cisco.com/web/about/citizenship/ethics/index.html (accessed September 4, 2012).

[4] Cisco, "Corporate Social Responsibility," www.cisco.com/web/about/citizenship/index.html (accessed September 4, 2012).

[5] Business Software Alliance, "Shadow Market: 2011 BSA Global Software Piracy Study," May 2012, http://portal.bsa.org/globalpiracy2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf (accessed November 20, 2012).

[6] Business Software Alliance, "Shadow Market: 2011 BSA Global Software Piracy Study," May 2012, http://portal.bsa.org/globalpiracy2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf (accessed November 20, 2012).

[7] Kim Zetter, "Madoff's Coders Charged with Aiding Massive Ponzi Scheme," *Wired*, November 13, 2009, www.wired.com/threatlevel/2009/11/madoff-programmers.

[8] Ketaki Gokhale, "Satyam Tumbles in Mumbai Trading After Posting Loss Amid Financial Probe," *Bloomberg.com*, September 30, 2010, www.bloomberg.com/news/2010-09-30/satyam-tumbles-in-mumbai-trading-after-company-reports-full-year-loss.html.

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

[10] Jessica Holzer and Shayndi Raice, "IBM Settles Bribery Charges," *Wall Street Journal*, March 19, 2011.

[11] Ben Rooney, "Online Poker Companies Indicted for Fraud," *CNN Money*, April 15, 2011, http://money.cnn.com/2011/04/15/news/economy/online_poker_indictments/index.htm.

[12] Shahien Nasiripour, "Citi 'Deficient' on Money Laundering Rules," *Financial Times*, April 6, 2012.

[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] Cammy Clark, "Florida Keys' Administrator Keeps Job After iPhone Scandal," *Miami Herald*, September 11, 2012, www.miamiherald.com/2012/09/10/2995966/florida-keys-administrator-keeps.html.

[15] Elizabeth Montalbano, "Government Eyeing Security Technology to Prevent Another Wikileaks," *InformationWeek*, March 21, 2011, www.informationweek.com/government/security/government-eyeing-security-technology-to/229301353.

[16] "Online Fraud Picks Up In 2011," *Internet Retailer*, May 1, 2012, www.internetretailer.com/2012/05/01/online-retail-fraud-picks-2011.

[17] Nina Kruschwitz, "How Intel Builds Sustainability Into the Bottom Line," *MIT Sloan Management Review*, May 25, 2012, www.greenbiz.com/blog/2012/05/25/how-intel-builds-sustainability-into-bottom-line.

[18] Jill Reilly, "What About Us?" *Mail Online*, April 3, 2012, www.dailymail.co.uk/news/article-2124429/What-Burger-King-unveils-healthier-food-menu-U-S-decides-leave-Brits-old-offerings.html.

[19] Dell Inc., "About Dell: Communities," http://content.dell.com/us/en/corp/dell-difference.aspx?c=us&l=en&s=corp&~ck=mn#! (accessed October 21, 2012).

[20] Ariel Swartz, "The Secrets Behind Google's Push Into Renewable Power," *Co.Exist*, www.fastcoexist.com/1677936/the-secrets-behind-googles-push-into-renewable-power (accessed October 20, 2012).

[21] IBM, "2011 Corporate Responsibility Summary," www.ibm.com/ibm/responsibility/2011/bin/downloads/IBM_Corp_Responsibility_Report_2011.pdf (accessed October, 20, 2012).

[22] Oracle, "Corporate Citizenship Report: Positive Impact," www.oracle.com/us/corporate/citizenship/index.html (accessed October 20, 2012).

[23] SAP AG, "Social Investment: Creating Opportunity for People Throughout the World," www.sap.com/corporate-en/sustainability/corporate-social-responsibility.epx (accessed October 20, 2012).

[24] Microsoft Corporation, "Corporate Citizenship: Employee Giving," www.microsoft.com/about/corporatecitizenship/en-us/serving-communities/disaster-and-humanitarian-response/employee-giving (accessed October, 20, 2012).

[25] Laura Matthews, "Excederin 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] John Foley, "Amid Contract Scandal, A Shakeup and Lingering Questions," *Information-Week*, October 22, 2010, www.informationweek.com/news/government/policy/showArticle.jhtml?articleID=227900598.

[28] David Hubler, "GTSI to be Sold to Unicom for $76.67M," May 7, 2012, *Washington Technology*, http://washingtontechnology.com/articles/2012/05/07/gtsi-sale-unicom.aspx.

[29] Paula, J. Desio, "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).

[30] Sharon Gaudin, "Bad Press May Affect Google More Than FTC's $22.5 Million Fine," *ComputerWorld*, August 9, 2012, www.computerworld.com/s/article/9230149/Bad_press_may_affect_Google_more_than_FTC_s_22.5M_fine.

[31] Ethics Resource Center, "2011 National Business Ethics Survey: Workplace Ethics in Transition," www.ethics.org/news/new-research-2011-national-business-ethics-survey (accessed October 19, 2012).

[32] Ethics Resource Center, "2011 National Business Ethics Survey: Workplace Ethics in Transition," www.ethics.org/news/new-research-2011-national-business-ethics-survey (accessed October 19, 2012).

[33] "What is an Ethics Officer?," *WiseGEEK*, www.wisegeek.com/what-is-an-ethics-officer.htm (accessed November 21, 2012).

[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] Yinka Adegoke, "News Corp Sets Up Global Ethics Team in Wake of Hacking Scandal," Reuters, August 15, 2012, www.reuters.com/article/2012/08/15/us-newscorp-idUSBRE87E0SH20120815.

[38] Bob Tricker and Chris Mallin, "High Corporate Governance Standards: Low Ethical Performance (the NewsCorp Case)," *Corporate Governance* (blog), September 8, 2011, http://corporategovernanceoup.wordpress.com/2011/09/08/high-corporate-governance-standards-low-ethical-performance-the-newscorp-case.

[39] Kate Benner, "Is Sarbanes Oxley a Failure?," *Fortune*, March 24, 2010.

[40] "CR's 100 Best Corporate Citizens 2012," *Corporate Responsibility*, www.thecro.com/files/100Best2012_List_3.8.pdf (accessed October 20, 2012).

[41] Samantha Neary, "Intel Reduces GHG Emissions by 60% Under 2007 Baseline," *Triple Pundit*, June 14, 2012, www.triplepundit.com/2012/06/intel-inside-intel-publishes-2012-corporate-responsibility-report.

[42] Ethics Resource Center, "2011 National Business Ethics Survey: Workplace Ethics in Transition," www.ethics.org/news/new-research-2011-national-business-ethics-survey (accessed October 19, 2012).

[43] Audra Bianca, "Ethics Awareness Training," *eHow*, www.ehow.com/about_6574961_ethics-awareness-training.html (accessed October 20, 2012).

[44] Motorola, "Corporate Responsibility: Business Conduct," http://responsibility.motorola.com/index.php/overview/busconduct/#ethics (accessed on October 20, 2012).

[45] "Fortune 500: 1976 Full List," *CNNMoney*, http://money.cnn.com/magazines/fortune/fortune500_archive/full/1976 (accessed October 23, 2012).

[46] IBM, "2011 IBM and the Environment Report," www.ibm.com/ibm/environment/annual/IBMEnvReport_2011.pdf (accessed October 22, 2012).

[47] IBM, "2011 Corporate Responsibility Summary," www.ibm.com/ibm/responsibility/2011/bin/downloads/IBM_Corp_Responsibility_Report_2011.pdf (accessed October 22, 2012).

[48] "Fortune 500: 2012 Full List," *CNNMoney*, http://money.cnn.com/magazines/fortune/fortune500/2012/full_list (accessed November 20, 2012).

[49] IBM, "2011 IBM and the Environment Report," www.ibm.com/ibm/environment/annual/IBMEnvReport_2011.pdf (accessed October 22, 2012).

[50] IBM, "2011 Corporate Responsibility," www.ibm.com/ibm/responsibility/2011/bin/downloads/IBM_Corp_Responsibility_Report_2011.pdf (accessed October 22, 2012).

[51] IBM, "2011 Corporate Responsibility," www.ibm.com/ibm/responsibility/2011/bin/downloads/IBM_Corp_Responsibility_Report_2011.pdf (accessed October 22, 2012).

[52] T.C. Sottek, "Nokia's New PureView Ad Is Amazing, Too Bad It's Faked," September 5, 2012, www.theverge.com/2012/9/5/3294545/nokias-pureview-ads-are-fraudulent.

[53] Michael Zhang, "Nokia Caught Faking PureView Floating Lens Stabilization in Promo Video," September 5, 2012, www.petapixel.com/2012/09/05/nokia-caught-faking-floating-lens-stabilization-in-promo-video/#GuPw9E6fzsb5ArfA.99.

[54] Tom Warren, "Nokia Issues Full Apology for Faked Lumia PureView Ad, Provides Real Footage," September 5, 2012, www.theverge.com/2012/9/5/3295316/nokia-apology-lumia-pureview-ad.

[55] Adam Ewing, "Nokia to Conduct Ethics Review Into Misleading Ad Video," *Bloomberg Businessweek*, September 10, 2012, www.businessweek.com/news/2012-09-10/nokia-to-conduct-ethics-review-about-misleading-ads.

[56] Dan Gallagher, "Nokia Confirms 'Poor Judgment'; Shares Jump," *MarketWatch*, www.marketwatch.com/story/nokia-confirms-poor-judgment-shares-jump-2012-09-14.

[57] Geraldine Willigan, "Nokia: Values that Make a Company Global," *Society for Human Resource Management*, 2009, www.shrm.org/Education/hreducation/Documents/Nokia_Values_Case_with%20teaching%20notes.pdf (accessed December 19, 2012).

[58] "Factory Closure: German State Demands €60 Million from Nokia," *Der Spiegel*, March 11, 2008, www.spiegel.de/international/business/factory-closure-german-state-demands-60-million-from-nokia-a-540699.html.

[59] "German Politicians Return Cell Phones Amid Nokia Boycott Calls. January 18, 2008, *DW*, www.dw.de/german-politicians-return-cell-phones-amid-nokia-boycott-calls/a-3076534-1.

[60] Adam Taylor, "Anger In Romania After Nokia Announces Factory To Close," *Business Insider International*, September 29, 2011, www.businessinsider.com/nokia-job-cuts-roju-cluj-romania-3500-2011-9.

[61] Rory Cellan-Jones, "Hi-Tech Helps Iranian Monitoring," *BBC News*, June, 22, 2009, http://news.bbc.co.uk/2/hi/technology/8112550.stm.

[62] Rory Cellan-Jones, "Hi-Tech Helps Iranian Monitoring," *BBC News*, June, 22, 2009, http://news.bbc.co.uk/2/hi/technology/8112550.stm.

[63] Rory Cellan-Jones, "Hi-Tech Helps Iranian Monitoring," *BBC News*, June, 22, 2009, http://news.bbc.co.uk/2/hi/technology/8112550.stm.

[64] Saeed Kamali Dehghan, "Iranian Consumers Boycott Nokia for 'Collaboration,'" *The Guardian*, July 14, 2009, www.guardian.co.uk/world/2009/jul/14/nokia-boycott-iran-election-protests.

[65] EUobserver, "Nokia-Siemens Rues Iran Crackdown Role," *Bloomberg Businessweek*, June 3, 2010, www.businessweek.com/globalbiz/content/jun2010/gb2010063_509207.htm.

[66] Steve Stecklow, "Nokia Siemens Venture to Reduce Its Business in Iran," *Wall Street Journal*, December 14, 2011, http://online.wsj.com/article/SB10001424052970203430404577096503401073904.html.

[67] Eija Warma, "'Lex Nokia' and Confidentiality In Electronic Communications in Finland," *Technology Law Section/State Bar of Georgia*, July 26, 2012, http://technologybar.org/2010/07/%E2%80%9Clex-nokia%E2%80%9D-and-confidentiality-in-electronic-communications-in-finland.

[68] Tamro Virki, "Nokia's U.S. Ambitions Hit by Smartphone Bug," *thestar.com*, April 11, 2012, www.thestar.com/business/article/1159515—nokia-s-u-s-ambitions-hit-by-smartphone-bug.

[69] Leslie D'Monte, "Nokia Fights Back as Samsung Eats into India Handset Share," *Live Mint*, May 14, 2012, www.livemint.com/Industry/jsKoeIaYRb2itvLBXmy2KM/Nokia-fights-back-as-Samsung-eats-into-India-handset-share.html.

[70] Michael Schrage, "Ethics, Shmethics," *CIO*, April 5, 2005, www.cio.com.au/article/185611/ethics_shmethics.

CHAPTER 2

ETHICS FOR IT WORKERS AND IT USERS

QUOTE

This above all: to thine own self be true.
—William Shakespeare, playwright

VIGNETTE

New York City Payroll Project Riddled with Fraud

The CityTime project was meant to replace a largely manual, paper-based payroll system for the city of New York (NYC). The goal was to provide a tool that would help city administrators manage a workforce of over 100,000 employees spread across 63 departments. It was also intended to simplify the employee time-reporting process, which was complicated by numerous union timekeeping rules, and to identify employees who tried to fraudulently inflate their paychecks. The project was initiated in 1998 when the city awarded the contract to a subsidiary of MCI, a telecommunications company that later ran into financial scandals and, ultimately, filed for bankruptcy.[1]

In 2001, the CityTime contract was reassigned to Science International Applications Incorporated (SAIC), a defense company. In an unusual move, the handoff to SAIC occurred without the contract going through the normal competitive bidding process required for contracts of this size. Around the same time, Spherion Atlantic Enterprises was hired as a subcontractor to provide quality assurance

on the CityTime project, with an initial contract of $3.4 million. The city's contract with Spherion was eventually revised 11 times, with a resulting cost of $48 million.[2]

Richard Valcich, the NYC payroll office executive director during the initial years of the project, accused SAIC of dragging its feet on the project and was skeptical of the company's ability to deliver a quality product. However, Valcich retired in 2004 and was replaced by Joel Bondy, a staunch advocate of the project.[3] In this role, Bondy was responsible for overseeing and re-awarding Spherion's contract. It was later discovered that Bondy worked for Spherion for two years prior to joining the city.

In another questionable move, the CityTime contract was switched from a fixed-price contract to a "time and materials" contract, and the project costs spiraled out of control—from $224 million in 2006 to $628 million by 2009. This switch in the terms of the contract plus lack of project oversight made it even easier for those involved with the project to commit fraud.[4]

At a city hearing in December 2010, Bondy revealed that Spherion employees were billing the city at a rate of $236.25 per hour and that a number of former city employees had become Spherion employees.[5] Mr. Bondy resigned shortly after this meeting.[6]

That same month, federal prosecutors charged several consultants for the CityTime project with a multimillion dollar fraud scheme, which allegedly started in 2005. The consultants were accused of manipulating the city into paying for contracts to businesses that the consultants controlled, and then redirecting part of the money to enrich themselves personally.[7]

In May 2011, federal investigators arrested Gerald Denault, the senior project manager at SAIC, for allegedly receiving over $5 million in kickbacks and for committing wire fraud and money laundering. Denault had convinced his employer to hire TechnoDyne LLC as the main subcontractor for the

project. TechnoDyne eventually received $450 million out of the $600 million paid to SAIC and siphoned off millions to a bogus India-based consulting firm owned by Denault.[8] The two owners of TechnoDyne are now fugitives and their whereabouts are unknown. Six other defendants are scheduled to go to trial in 2013.[9]

In March 2012, SAIC agreed to pay $500 million to avoid prosecution for its role in the CityTime scandal; most of that money was to go back to the city of New York. By this time, it was estimated that NYC had paid out $652 million—with an outstanding bill of $41 million—owed on the project, which was originally estimated to cost $63 million and to be completed in 2003.[10]

Questions to Consider

1. What were some early warning signs that signaled things were not going well with the CityTime project?
2. What steps should city managers and SAIC have taken at an early stage of the project to identify and prevent fraud?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What key characteristics distinguish a professional from other kinds of workers, and is an IT worker considered a professional?
2. What factors are transforming the professional services industry?
3. What relationships must an IT worker manage, and what key ethical issues can arise in each?
4. How do codes of ethics, professional organizations, certification, and licensing affect the ethical behavior of IT professionals?
5. What is meant by compliance, and how does it help promote the right behaviors and discourage undesirable ones?

IT PROFESSIONALS

A **profession** is a calling that requires specialized knowledge and often long and intensive academic preparation. Over the years, the United States government adopted labor laws and regulations that required a more precise definition of what is meant by a *professional*

employee. The United States Code of federal regulations defines a "professional employee" as one who is engaged in the performance of work:

> "(i) requiring knowledge of an advanced type in a field of science or learning customarily acquired by a prolonged course of specialized intellectual instruction and study in an institution of higher learning or a hospital (as distinguished from knowledge acquired by a general academic education, or from an apprenticeship, or from training in the performance of routine mental, manual, mechanical, or physical activities);
> (ii) requiring the consistent exercise of discretion and judgment in its performance;
> (iii) which is predominantly intellectual and varied in character (as distinguished from routine mental, manual, mechanical, or physical work); and
> (iv) which is of such character that the output produced or the result accomplished by such work cannot be standardized in relation to a given period of time."[11]

In other words, professionals such as doctors, lawyers, and accountants require advanced training and experience; they must exercise discretion and judgment in the course of their work; and their work cannot be standardized. Many people would also expect professionals to contribute to society, to participate in a lifelong training program (both formal and informal), to keep abreast of developments in their field, and to assist other professionals in their development. In addition, many professional roles carry special rights and responsibilities. Doctors, for example, prescribe drugs, perform surgery, and request confidential patient information while maintaining doctor–patient confidentiality.

Are IT Workers Professionals?

Many business workers have duties, backgrounds, and training that qualify them to be classified as professionals, including marketing analysts, financial consultants, and IT specialists such as mobile application developers, software engineers, systems analysts, and network administrators. One could argue, however, that not every IT role requires "knowledge of an advanced type in a field of science or learning customarily acquired by a prolonged course of specialized intellectual instruction and study," to quote again from the United States Code. From a *legal* perspective, IT workers are not recognized as professionals because they are not licensed by the state or federal government. This distinction is important, for example, in malpractice lawsuits, as many courts have ruled that IT workers are not liable for malpractice because they do not meet the legal definition of a professional.

Professional Relationships That Must Be Managed

IT workers typically become involved in many different relationships, including those with employers, clients, suppliers, other professionals, IT users, and society at large—as illustrated in Figure 2-1. In each relationship, an ethical IT worker acts honestly and appropriately. These various relationships are discussed in the following sections.

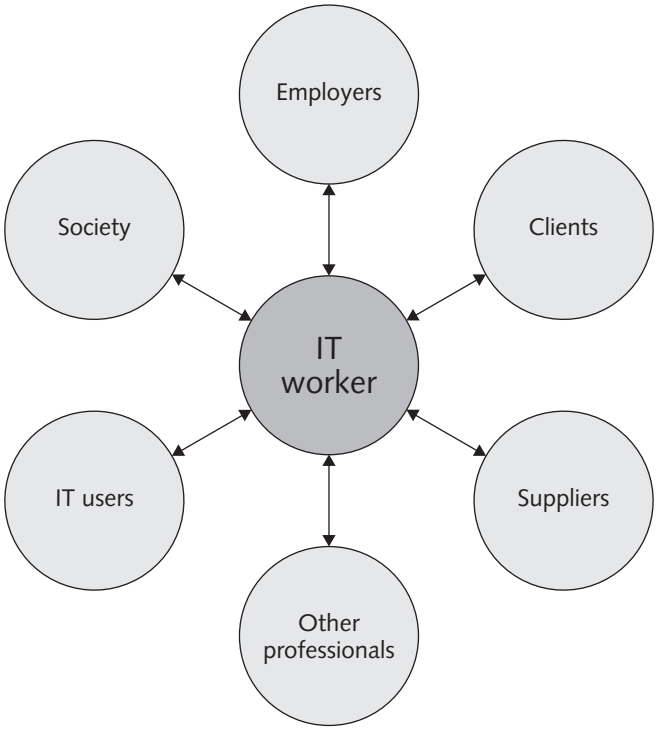


FIGURE 2-1 Professional relationships IT workers must manage
Credit: Course Technology/Cengage Learning.

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 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. These issues may include protection of company secrets; vacation policy; time off 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 as the need arises (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 aspects 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 **Business Software Alliance (BSA)** is a trade group that represents the world's largest software and hardware manufacturers. Its mission is to stop the unauthorized copying of software produced by its members. BSA is funded both through dues based on member companies' software revenues and through settlements from companies that commit piracy. BSA membership includes two dozen or so members such as Adobe, Apple, Intel, McAfee, Microsoft, Symantec, and The Math Works.

More than 100 BSA lawyers and investigators prosecute thousands of cases of software piracy each year. BSA investigations are usually triggered by calls to the BSA hotline (1-888-NO-PIRACY), reports sent to the BSA Web site (*www.nopiracy.org*), and referrals from member companies. Many of these cases are reported by disgruntled employees or former employees. For 2011, the commercial value of software piracy in the United States was estimated to be nearly $10 billion with 31 percent of computer users participating in this illegal activity.[12] When BSA finds cases of software piracy, it assesses heavy monetary penalties.

Failure to cooperate with the BSA can be extremely expensive. The cost of criminal or civil penalties to a corporation and the people involved can easily be many times more expensive than the cost of "getting legal" by acquiring the correct number of software licenses. Software manufacturers can file a civil suit against software pirates with penalties of up to $150,000 per copyrighted work. Furthermore, the government can criminally prosecute violators and fine them up to $250,000, incarcerate them for up to five years, or both.

In 2012, the Alexander Automotive Group paid $325,000 to settle claims that it was using unlicensed Microsoft software on its computers. As part of the settlement agreement with BSA, the firm deleted all unlicensed copies of software from its computers, purchased the licenses required to become compliant, and agreed to implement more effective software management procedures. BSA was alerted to this situation by a report sent to its Web site.[13]

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 i7 quad 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.

Zynga is a provider of online social games such as ChefVille, CityVille, FarmVille, FrontierVille, and Zynga Poker that boast over 300 million active monthly users.[14] After just over a year with Zynga, the firm's general manager of CityVille left to become a vice president at Kixeye, a competitor. Zynga claimed that the employee stole files with data critical to the business—including financial projections, marketing plans, and game designs.[15] Zynga filed a request for a temporary restraining order barring its former employee from sharing or copying the information or from engaging in any actions using the information to develop online games employing these trade secrets.

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 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.

The H-1B visa is a work visa that allows foreigners to come to the United States and work full-time in specialty occupations that require at least a four-year bachelor's degree in a specific field. A U.S. consultant for India-based outsourcing firm Infosys filed a whistle-blower lawsuit against the firm for abusing H-1B program rules. The lawsuit alleged that at a management meeting in Bangalore, Infosys officials discussed the need to "creatively" circumvent the H-1B visa restrictions. The lawsuit further alleged that Infosys brought workers to the United States on B-1 visas (which are intended for workers coming to the United States for short-term work assignments only), but that these workers were assigned full-time jobs. It also claimed that Infosys was not paying the B-1 workers the prevailing wage and was not withholding federal and state income taxes.[16] The whistle-blower filed a separate lawsuit in which he claimed that Infosys retaliated against him for the filing of the visa-related lawsuit by lowering his bonuses, harassing him, and giving him no meaningful work to do.[17]

Relationships Between IT Workers and Clients

IT workers provide services to clients; sometimes those "clients" are coworkers who are part of the same organization as the IT worker. In other cases, the client is part of a different organization. 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 client and 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 interests of the client. 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 whether its recommendations can be trusted.

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.

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.

As an example of alleged fraud, consider the case of Paul Ceglia, who in 2010 sued Facebook claiming to own a majority of the company. Ceglia claimed that he signed a contract with Mark Zuckerberg in 2003 to design and develop the Web site that eventually became Facebook. He alleged that he paid Zuckerberg $1,000 for the programming work and also invested an additional $1,000 in Zuckerberg's Facebook project in exchange for a 50 percent interest in Facebook.[18] Facebook lawyers have asserted that the lawsuit is an outright fraud and have depositions alleging that "Ceglia manufactured evidence, including purported emails with Zuckerberg, to support his false claim to an interest in Facebook" and that "Ceglia destroyed evidence that was inconsistent with his false claim." Facebook's attorneys pointed out that Zuckerberg did not even conceive of Facebook until eight

months after Zuckerberg did the contract work (which, they say, was completely unrelated to Facebook) for Ceglia. They further alleged that Ceglia's emails to Zuckerberg were manufactured to support his claims. Eventually, Ceglia was arrested on federal mail and wire fraud charges.[19]

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.

Siri, the voice-activated software that comes with the Apple iPhone, has delighted many iPhone users; however, not everyone has had a positive experience. Shortly after one user in New York purchased an iPhone 4S, he realized that Siri was not performing as expected. When he asked Siri for directions, it did not understand the question or after a long delay gave incorrect directions. As a result, the user filed a lawsuit against Apple claiming that advertising for the Siri amounted to "intentional misrepresentation" and that Apple's claims about the Siri software were "misleading and deceptive." Attorneys for this user are considering turning the case into a class action against Apple.[20]

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 nonbreaching 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."[21]

In an out-of-court settlement of a breach of contract lawsuit brought by the General Services Administration (GSA), Oracle Corporation agreed to pay the federal agency $200 million. Oracle entered into a contract with the GSA for the sale of software and technical support to various departments of the federal government. The contract required Oracle to provide the government with its pricing policies. The lawsuit arose when the GSA claimed that Oracle "knowingly failed to meet its contractual obligations to provide GSA with current, accurate, and complete information about its commercial sales practices, including discounts offered to other customers, and that Oracle knowingly made false statements to GSA about its sales practices and discounts." The GSA further claimed that Oracle failed to disclose that other customers received greater discounts than the GSA and that, based on its contract with Oracle, those discounts should have been passed on to the GSA.[22]

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. Consider the following frequent causes of problems in IT projects:

- The customer changes the scope of the project or the system requirements.
- Poor communication between customer and vendor leads to performance that does not meet expectations.
- The vendor delivers a system that meets customer requirements, but a competitor comes out with a system that offers more advanced and useful features.
- The customer fails to reveal information about legacy systems or databases that make the new system extremely difficult to implement.

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.

A former midlevel supply chain manager at Apple pled guilty in 2011 to taking over $1 million in payments from certain iPhone, iPad, and iPod suppliers in China, Singapore, South Korea, and Taiwan. The kickbacks took place over several years and were in exchange for the employer providing confidential information about Apple's production plans, enabling the suppliers to negotiate more favorable deals with Apple. He now faces 20 years in prison on charges of money laundering, receiving kickbacks, and wire fraud.[23]

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. 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 five years.

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 controls, including maintaining books and records that accurately and fairly reflect their transactions. 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 frequently audited by both internal and outside auditors to ensure that they meet these standards.

The FCPA permits facilitating payments that are made for "routine government actions," such as obtaining permits or licenses; processing visas; providing police protection; providing phone services, power, or water supplies; or facilitating actions of a similar nature. Thus, it is permissible under the FCPA to pay an official to perform some official function faster (for example, to speed customs clearance) but not to make a different substantive decision (for example, to award business to one's firm).[24]

There is growing global recognition of the need to prevent corruption. The United Nations Convention Against Corruption is a legally binding global treaty designed to fight bribery and corruption. During its November 2010 meeting, Finance Ministers and Central Bank Ministers of members of the Group of 20 (G20), which includes Argentina, China, India, Japan, Russia, the United Kingdom, the United States, and 13 other countries, pledged to implement this treaty effectively. In particular, the countries pledged to put in place mechanisms for the recovery of property from corrupt officials through international cooperation in tracing, freezing, and confiscating assets. Members also pledged to adopt and enforce laws against international bribery and put in place rules to protect whistleblowers.[25]

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 some 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

Source Line: Course Technology/Cengage Learning.

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.

Yahoo! hired Scott Thompson, the president of eBay's PayPal electronic payments unit, as its new CEO in January 2012.[26] Just four months later, Thompson left the company, due, at least in part, to revelations that his résumé falsely claimed that he had earned a bachelor's degree in computer science.[27]

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.[28] Résumé inflation is an even bigger problem in Asia. According to a recent survey conducted by the University of Hong Kong and a Hong Kong–based company specializing in preemployment screening, over 62 percent of respondents confessed to exaggerating their years of experience, previous positions held, and job responsibilities; 33 percent confessed to having exaggerated even more.[29] 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	How to uncover the truth
Dates of employment	Thorough reference check
Job title	Thorough reference check
Criminal record	Criminal background check
Inflated salary	Thorough reference check
Education	Verification of education claims with universities and other training organizations
Professional licenses	Verification of license with accrediting agency
Working for fictitious company	Thorough background check

Source Line: Lisa Vaas, "Most Common Resume Lies," The Ladders, July 17, 2009, www.theladders.com/career-advice/most-common-resume-lies.

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.

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. IT workers also have a key responsibility to establish an environment that supports ethical behavior 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 residents 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.

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. Just because an activity is not defined as illegal does not mean it is ethical. 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 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, Web sites, 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) is a computing society founded in 1947 with over 97,000 student and professional members in more than 100 countries. It is international in scope—with an ACM Europe, ACM India, and ACM China organization. ACM currently publishes over 50 journals and magazines and 30 newsletters—including *Communications of the ACM* (ACM's primary publication), *ACM Tech News* (coverage of timely topics for IT professionals), *XRDS* (for both graduate and undergraduate students considering computing careers), *RISKS Forum* (a moderated dialogue on risks to the public from computers and related systems), and *eLearn* (an online magazine about online education and training). The organization also offers a substantial digital library of bibliographic information, citations, articles, and journals. The ACM sponsors 37 special-interest groups (SIGs) representing major areas of computing. Each group provides publications, workshops, and conferences for information exchange.[30]

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 85,000 members. Founded in 1946, the IEEE-CS is the largest of the 38 societies of the IEEE. The IEEE-CS helps meet the information and career development needs of computing researchers and practitioners with technical journals, magazines, books, conferences, conference publications, and online courses. It also offers a Certified Software Development Professional (CSDP) program for experienced professionals and a Certified Software Development Associate (CSDA) credential for recent college graduates. The society sponsors many conferences, applications-related and research-oriented journals, local and student chapters, technical committees, and standards working groups.[31]

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 "Software Engineering Code of Ethics and Professional Practice"

documents the ethical and professional responsibilities and obligations of software engineers. After a thorough review process, version 5.2 of the Software Engineering Code of Ethics was adopted by both the ACM and IEEE-CS in 1999.[32]

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.[33]

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.

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.[34]

At no cost, SANS makes available a collection of some 1,200 research documents about various topics of information security. 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.

Table 2-3 provides the URL for the codes of ethics for the above IT professional organizations.

TABLE 2-3 Code of ethics for popular IT professional organizations

Organization	URL for code of ethics
Association for Computing Machinery	www.acm.org/about/code-of-ethics
Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS)	http://seeri.etsu.edu/Codes/TheSECode.htm
Association of Information Technology Professionals (AITP)	www.aitp.org/?page=Ethics
SysAdmin, Audit, Network, Security (SANS) Institute	www.sans.org/security-resources/ethics.php

Source Line: Course Technology/Cengage Learning.

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 (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. 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. Is certification relevant to your current job or the one to which 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.

Industry Association Certifications

There are many available industry certifications in a variety of IT-related subject areas. Their value varies greatly depending on where people are in their career path, what other certifications they possess, and the nature of the IT job market. Table 2-4 lists several of the certifications most in demand by employers.

TABLE 2-4 Certifications in high demand

Certification	Subject matter
Microsoft Certified Technology Specialist	Designing and optimizing solutions based on Microsoft products and technologies
Cisco Certified Internetwork Expert	Managing and troubleshooting large networks
Cisco Certified Network Professional Security	Configuring and designing firewalls and the security settings on routers and switches
CompTIA A+	Performing computer and network maintenance, troubleshooting, and installation—including addressing security issues
Project Management Institute's Project Management Professional (PMP)	Leading and directing projects

Source Line: Course Technology/Cengage Learning.

Certification requirements generally oblige an individual to have the prerequisite education and experience, and to sit for and pass an exam. In order to remain certified, the individual must typically pay an annual certification fee, earn continuing education credits, and—in some cases—pass a periodic renewal test.

Certifications from industry associations generally require a higher level of experience and a broader perspective than vendor certifications; however, industry associations often lag in developing tests that cover new technologies. The trend in IT certification is to move from purely technical content to a broader mix of technical, business, and behavioral competencies, which are required in today's demanding IT roles. This trend is evident in industry association certifications that address broader roles, such as project management and network security.

Government Licensing

In the United States, a **government license** is government-issued permission to engage in an activity or to operate a business. It 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.

States have enacted legislation to establish licensing requirements and protect public safety in a variety of fields. For example, Texas passed the Engineering Registration Act after a tragic school explosion at New London, Texas, in 1937. Under the act and

subsequent revisions, only duly licensed people may legally perform engineering services for the public, and public works must be designed and constructed under the direct supervision of a licensed professional engineer. People cannot call themselves engineers or professional engineers unless they are licensed, and violators are subject to legal penalties. Most states have similar laws.

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. Highly integrated enterprise resource planning (ERP) systems help multibillion-dollar companies control all of their business functions, including forecasting, production planning, purchasing, inventory control, manufacturing, and distribution. Complex computers and information systems manage and control the nuclear reactors of power plants that generate electricity. Medical information systems monitor the vital statistics of hospital patients on critical life support. Every year, local, state, and federal government information systems are entrusted with generating and distributing millions of checks worth billions of dollars to the public.

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. Licensing would also allow for violators to be punished. Without licensing, there are no clear, well-defined requirements for heightened care and no concept of professional malpractice.

Issues Associated with Government Licensing of IT Workers

Australia, Great Britain, and the Canadian provinces of Ontario and British Columbia have adopted licensing for software engineers. In the United States, the National Council of Examiners for Engineering and Surveying (NCEES) has developed a professional exam for electrical engineers and computer engineers. However, there are many reasons why there are few international or national licensing programs for IT workers in the United States:

- *There is no universally accepted core body of knowledge*. The core **body of knowledge** for any profession outlines agreed-upon sets of skills and abilities that all licensed professionals must possess. At present, however, there are no universally accepted standards for licensing programmers, software engineers, and other IT workers. Instead, various professional societies, state agencies, and federal governments have developed their own standards.
- *It is unclear who should manage the content and administration of licensing exams*. How would licensing exams be constructed, and who would be responsible for designing and administering them? Would someone who passes a license exam in one state or country be accepted in another state or country? In a field as rapidly changing as IT, workers must commit to ongoing, continuous education. If an IT worker's license were to expire every few years (like a driver's license), how often would practitioners be required to prove competence in new practices in order to renew their license? Such

questions would normally be answered by the state agency that licenses other professionals.

- *There is no administrative body to accredit professional education programs*. Unlike the American Medical Association for medical schools or the American Bar Association for law schools, no single body accredits professional education programs for IT. Furthermore, there is no well-defined, step-by-step process to train IT workers, even for specific jobs such as programming. There is not even broad agreement on what skills a good programmer must possess; it is highly situational, depending on the computing environment.
- *There is no administrative body to assess and ensure competence of individual workers*. Lawyers, doctors, and other licensed professionals are held accountable to high ethical standards and can lose their license for failing to meet those standards or for demonstrating incompetence. The AITP standards of conduct state that professionals should "take appropriate action in regard to any illegal or unethical practices that come to [their] attention. However, [they should] bring charges against any person only when [they] have reasonable basis for believing in the truth of the allegations and without any regard to personal interest." The AITP code addresses the censure issue much more forcefully than other IT codes of ethics, although it has seldom, if ever, been used to censure practicing IT workers.

IT Professional Malpractice

Negligence has been 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 for employees.

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, Oracle-certified 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.

Courts have consistently rejected attempts to sue individual parties for computer-related malpractice. Professional negligence can only occur when people fail to perform within the standards of their profession, and software engineering is not a uniformly licensed profession in the United States. Because there are no uniform standards against which to compare a software engineer's professional behavior, he or she cannot be subject to malpractice lawsuits.

IT USERS

Chapter 1 outlined the general topic of how corporations are addressing the increasing risks of unethical behavior. This section focuses on encouraging employees' ethical use of IT, which is an area of growing concern as more companies provide employees with PCs, tablets, cellphones, and other devices to access to corporate information systems, data, and the Internet.

Common Ethical Issues for IT Users

This section discusses a few common ethical issues for 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. For example, the software piracy rate in China exceeds 80 percent, so it is clear that the business managers and IT professionals in that country do not take a strong stand against the practice.

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 Android Market Web site without paying for them, and then use the software or sell it to others. One legitimate Android application developer complained that his first application was pirated within a month and that the number of downloads from the pirate's site were greater than his own. Professional developers become discouraged as they watch their sales sink while pirates' sales rocket.[35]

Inappropriate Use of Computing Resources

Some employees use their computers to surf popular Web sites that have nothing to do with their jobs, participate in chat rooms, view pornographic sites, and play computer games. These activities eat away at worker 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.[36,37] Organizations typically fire frequent pornography offenders and take disciplinary action against less egregious offenders.

Recently, the executive director of the Pentagon's Missile Defense Agency issued a memo to its 8,000 employees warning them to stop using their work computers to access Internet porn sites. One concern of government officials is that many pornography sites are infected with computer viruses and other malware; criminals and foreign intelligence agencies often use such sites as a means to gain access to government and corporate computer networks. For example, a foreign agent can embed malware capable of stealing data or opening computer communications ports whenever certain photos or videos are downloaded to a computer.[38]

Inappropriate Sharing of Information

Every organization stores vast amounts of information that can be classified as either private or confidential. Private data describes individual employees—for example, their salary information, attendance data, health records, and performance ratings. Private data also includes 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.

In late 2010, hundreds of thousands of leaked State Department documents were posted on the WikiLeaks Web site. As of this writing, it appears that 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-scenes international diplomacy, often divulging candid comments from world leaders and providing particulars of U.S. tactics in Afghanistan, Iran, and North Korea.[39] The leaked documents strained relations between the United States and some of its allies. It is also possible that the incident will lead to less sharing of sensitive information with the United States because of concerns over further disclosures.

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 of the following actions when creating an IT usage policy.

Establishing Guidelines for Use of Company 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 the Appropriate Use of IT Resources

Companies must develop, communicate, and enforce written guidelines that encourage employees to respect corporate IT resources and use them to enhance their job performance. Effective guidelines allow some level of personal use while prohibiting employees from visiting objectionable Internet sites or using company email to send offensive or harassing messages.

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 that serves as a barrier 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 Web sites. (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 Web sites, 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.

Table 2-5 provides a manager's checklist for establishing an IT usage policy. The preferred answer to each questions is *yes*.

TABLE 2-5 Manager's checklist for establishing an IT usage policy

Question	Yes	No
Is there a statement that explains the need for an IT usage policy?		
Does the policy provide a clear set of guiding principles for ethical decision making?		
Is it clear how the policy applies to the following types of workers? • Employees • Part-time workers • 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, 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?		
Has a corporate firewall been implemented?		
Is the corporate firewall maintained and kept up to date?		

Source Line: Course Technology/Cengage Learning.

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 internal controls 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 to 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 is gathered, for what purposes the data is 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.[40]

Demonstrating compliance with multiple government and industry regulations, many with similar but sometimes conflicting requirements, can be a major challenge. As a result, many organizations have implemented specialized software to track and record compliance actions, hired management consultants to provide advice and training, and even created a new position, the chief compliance officer (CCO), to deal with the issues.

In 1972, the Securities and Exchange Commission (SEC) recommended that publicly held organizations establish audit committees.[41] 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 the 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 reported their findings to appropriate law enforcement agencies. For example, the audit committee of Sensata Technology (which designs, manufactures, and distributes electronic sensors and controls) conducted an investigation into whether certain company officials had violated foreign bribery laws in connection with a business deal in China. As a result of that investigation, the audit committee reported possible Foreign Corrupt Practices Act violations to the SEC and the Department of Justice.[42]

In addition to an audit committee, most organizations also have an internal audit department whose primary responsibilities are to

- Determine that internal systems and controls are adequate and effective
- Verify the existence of company 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.

The audit committee 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 the various organizational guidelines and policies as well as various legal and regulatory practices.

Summary

- The key characteristics that distinguish professionals from other kinds of workers are as follows: (1) They require advanced training and experience; (2) they must exercise discretion and judgment in the course of their work; and (3) their work cannot be standardized.
- 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.
- From a legal standpoint, a professional has passed the state licensing requirements (if they exist) and earned the right to practice there.
- From a legal perspective, IT workers are not recognized as professionals because they are not licensed by the state or federal government. As a result, IT workers are not liable for malpractice.
- IT professionals typically become involved in many different relationships, each with its own set of ethical issues and potential problems.
- In relationships between IT professionals 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 professionals and clients, key issues revolve around defining, sharing, and fulfilling each party's responsibilities for successfully completing an IT project.
- A major goal for IT professionals and suppliers is to develop good working relationships in which no action can be perceived as unethical.
- In relationships between IT workers, the priority is to improve the profession through activities such as mentoring inexperienced colleagues and demonstrating professional loyalty.
- Résumé inflation and the inappropriate sharing of corporate information are potential problems in relationships between IT workers.
- 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.
- A professional code of ethics states the principles and core values that are essential to the work of an occupational group.
- A code of ethics serves as a guideline for ethical decision making, promotes high standards of practice and ethical behavior, enhances trust and respect from the general public, and provides an evaluation benchmark.
- Several IT-related professional organizations have developed a code of ethics, including ACM, IEEE-CS, AITP, and SANS.
- 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.

- Many people believe that the licensing and certification of IT workers would increase the reliability and effectiveness of information systems.
- Licensing and certification raise many issues, including the following: (1) There is no universally accepted core body of knowledge on which to test people; (2) it is unclear who should manage the content and administration of licensing exams; (3) there is no administrative body to accredit professional education programs; and (4) there is no administrative body to assess and ensure competence of individual professionals.
- The audit committee 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

audit committee
body of knowledge
breach of contract
breach of duty of care
bribery
Business Software Alliance (BSA)
certification
compliance
conflict of interest
duty of care
firewall
Foreign Corrupt Practices Act (FCPA)
fraud
government license
IT user
material breach of contract
misrepresentation
negligence
profession
professional code of ethics
professional malpractice
reasonable person standard
reasonable professional standard
résumé inflation
trade secret
whistle-blowing

Self-Assessment Questions

The answers to the Self-Assessment Questions can be found in Appendix B.

1. A professional is someone who:
   a. requires advanced training and experience
   b. must exercise discretion and judgment in the course of his or her work
   c. does work that cannot be standardized
   d. all of the above
2. 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 members of the _____ organization.
3. The mission of the Business Software Alliance is to _____.

4. 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. True or False?
5. _____ is the crime of obtaining goods, services, or property through deception or trickery.
6. _____ means to be in accordance with established policies, guidelines, specifications, or legislation.
7. Society expects professionals to act in a way that:
   a. causes no harm to society
   b. provides significant benefits
   c. establishes and maintains professional standards that protect the public
   d. all of the above
8. Most organizations have a(n) _____ team with primary responsibilities to determine that internal systems and controls are adequate and effective.
9. _____ is a process that one undertakes voluntarily to prove competency in a set of skills.
   a. Licensing
   b. Certification
   c. Registration
   d. all of the above
10. Senior management (including members of the audit committee) has the option of ignoring or suppressing recommendations of the internal audit committee. True or False?
11. _____ has been defined as not doing something that a reasonable person would do, or doing something that a reasonable person would not do.
12. A(n) _____ states the principles and core values that are essential to the work of a particular occupational group.

Discussion Questions

1. Would you rather be known as a person of modest means with an impeccable ethical character or as an unscrupulous person of wealth? Why?
2. How do you distinguish between misrepresentation and embellishment of one's professional accomplishments on a résumé? Provide an example of an embellishment that would not be considered misrepresentation.
3. Do laws provide a complete guide to ethical behavior? Can an activity be legal but not ethical?
4. In filling an open position in a U.S.-based IT organization, 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?

5. Does charging by the hour encourage unethical behavior on the part of contract workers and consultants?
6. Describe a situation in which there could be a conflict of interest between an IT worker's self-interest and the interests of a client. How should this potential conflict be addressed?
7. Should all IT workers be either licensed or certified? Why or why not?
8. Go to two or more of the Web sites identified in Table 2-3, and read the code of ethics found there. What commonalities do you find among the IT professional codes of ethics that you read? What differences are there? Do you think there are any important issues not addressed by these codes of ethics?
9. 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 many occasions, you heard your boss make statements to this employee that could be interpreted as sexual advancements. 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. On the other hand, it was clear to you 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? Does it really matter if the case is dismissed because of your testimony?
10. What is the difference between breach of contract and material breach of contract? In a breach of contract dispute, what recourse can the nonbreaching party take?
11. Under the Foreign Corrupt Practices Act, under what conditions is a bribe not unlawful? Explain, and provide an example.

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 salesperson at a large software manufacturing firm. It is three weeks from the end of the sales quarter and you and your sales manager are sitting pretty—you have both already met your sales quota for the quarter. In addition, you just closed another deal with a new customer for $100,000 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?
2. You work part-time evenings and weekends as a real estate salesperson. You also work full-time for an IT consulting group. When ordering business cards for your real estate business, you decided to include your full-time work email address. As a result, you frequently find yourself receiving and sending emails related to your real estate work from your computer at your IT consulting job. You try to limit this activity to your lunch hour, but

there are often urgent messages that require an immediate reply. Lately the number of such emails is increasing. Sometimes you worry what would happen if your manager found out about this activity, but cutting off the flow of emails from your clients could have a serious impact on your ability to serve them and earn commissions. What should you do?

3. 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?
4. The daughter of the firm's CEO is scheduled to participate in a job interview for an entry-level position in the IT organization next week. You are a second-year employee in your firm's IT organization who will participate in the interview process. You will be one of three people who will interview her to form an assessment and make a group decision about whether or not she will be offered the position. How do you handle this situation?
5. 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 exchanged ideas about family vacations. You mentioned that your family is planning on vacationing in the Scottsdale, Arizona, area. You are surprised when the contractor emails you an offer to use his company's condominium at a plush Scottsdale resort, complete with golf and health club privileges. He assures you that the condo would normally be empty that time of year and that other customers frequently use the condo. The resort is one you are familiar with but have never used because the rental is well over $5,000 per week. You would really like for your family to experience staying at a five-star resort but you worry about the potential consequences of accepting the offer. If your manager saw a copy of the emails exchanged with the contractor, could it appear that you were soliciting a bribe? Could this offer be considered a bribe? What would you do?
6. Your organization is preparing to submit a bid for a multimillion-dollar contract in South America. The contract is extremely important to your firm and would represent its first contract in South America. While meeting with your South American contacts, you are introduced to a consultant who offers to help your firm prepare and submit its bid, as well as to negotiate with the prospective customer company. The consultant is quite impressive in his knowledge of local government officials and managers and executives at the customer's company. The fee requested is only 1 percent of the potential value of the contract, but it is unclear exactly what the consultant will do. Later that day, your local contacts tell you that the use of such consultants is common. They say that they are familiar with this particular consultant and that he has a good reputation for getting results. Your company has never worked with such consultants in the past, and you are uncertain on how to proceed. What would you do?
7. 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 organization. You are in

the process of reviewing more than 100 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 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?

Cases

1. Whistle-Blower Claims Accounting Shenanigans at SuccessFactors

SuccessFactors is a U.S. multinational company that provides cloud-based human resources-related software applications. Under its "software-as-a-service" business model, the company provides software resources to subscribers who access them via the Internet for a fee. Annual revenue for the firm was $206 million in 2010.[43]

SuccessFactors spreads its costs over a large number of subscribers to keep its subscription rates low and generate income. Subscribers, in turn, rely on SuccessFactors to manage their data and software in a secure and reliable manner. Subscribers avoid large capital outlays for computing equipment and eliminate the costs associated with the purchase of hardware and software and the hiring of numerous computer operations and support people.

SuccessFactors has not been profitable—incurring losses in each fiscal period since its inception in 2001, with a loss of $12.5 million for 2010 and an accumulated deficit of $231.3 million.[44] Nevertheless, SAP paid $3.4 billion (over 10 times its 2011 revenue of $327 million) to acquire SuccessFactors in early 2012. (This number compares very unfavorably with the median price—three times revenue—paid in the 32 software mergers that occurred in North America in the five years prior to SAP's purchase of SuccessFactors.)[45] SAP was willing to pay such a premium to gain significant market share and expertise in the rapidly growing human resources software-as-a-service arena. At the time, SuccessFactors had a customer base of some 15 million subscription seat licenses spread across 3,500 customers.[46]

As with many companies, SuccessFactors supplemented the financial results that it reported in accordance with GAAP (generally accepted accounting principles that form the basis for financial reporting), with non-GAAP financial measures. The manner in which such non-GAAP measures are defined and calculated differ from company to company.[47] One of these non-GAAP financial measures was a measure called "backlog." SuccessFactors, and many other cloud computing service firms, invoice subscribers on an annual basis even if the term of the subscription agreement is longer than one year. Amounts that have been invoiced, but that have not yet been recognized as revenue, are recorded as deferred revenue. SuccessFactors reported the portion of the total contract value not yet invoiced as backlog.[48] SuccessFactors had a backlog of about $90 million at the end of 2007 compared with a backlog of $43 million at the end of 2006—an increase the company attributed to an upsurge in new contracts and customers.[49] In 2009, SuccessFactors stopped reporting this backlog figure, and the omission caught the eye of the SEC. When the agency inquired about why the company was no longer

reporting this figure, SuccessFactors responded that it felt investors did not consider this figure useful.[50]

In the third quarter of 2010, Success Factors stated that it had adopted a 2009 SEC rule that limited the manner in which revenue could be reported on multiyear contracts.[51] However, in its 2011 annual report, filed just after SAP announced its intent to acquire the firm, but before the deal was finalized, SuccessFactors admitted that its accounting controls suffered from "a material weakness" and that its "internal control over financial reporting was not effective as of December 31, 2011."[52] Indeed, a SuccessFactors salesperson turned whistle-blower claimed that from 2009 to 2011, accounting controls at SuccessFactors were so weak that salespeople were able to improperly rewrite existing multiyear contracts as new contracts to earn additional commissions. If true, this would also accelerate revenue, making the company look more financially sound, while also reducing the backlog number. SAP investigated these claims with an examination conducted by an outside law firm and found no merit to the claims.[53]

Discussion Questions

1. In the end, SuccessFactors investors were not hurt by this alleged improper accounting because SAP paid such a high premium to acquire the firm, which helped SAP jump-start its cloud computing business. Was anyone hurt by this alleged improper accounting and, if so, who and how?
2. Should management encourage the reporting of non-GAAP financial measures that may be useful to investors? Why or why not?
3. What sort of measures should the management teams of service companies put in place to ensure that there is no improper accounting of multiyear contracts?

2. IBM and the State of Indiana Involved in a Breach of Contract Dispute

In December 2006, IBM and the Indiana Family and Social Services Administration (FSSA) entered into a 10-year, $1.16 billion contract to modernize the state's processes and systems for determining welfare eligibility. The state expected to generate $500 million in administrative costs savings over the life of the contract.[54]

FSSA claims it began to notice problems in the new system as early as the project's initial rollout to 10 northern Indiana counties in October 2007. As a result, further expansion was delayed. The state's lawyers wrote: "IBM assured FSSA that if the Region 2 rollout was implemented, IBM would recognize some efficiencies and economies of scale that would improve performance." Accordingly, FSSA agreed to roll out the system to the next region.[55]

By May 2008, the system had expanded into 59 of Indiana's 92 counties. In January 2009, a new FSSA secretary Anne Murphy took over and halted any further expansion until IBM submitted a corrective action plan. She set a deadline of July 2009, and her request included the stipulation that the contract be canceled if IBM failed to improve the situation by September 2009.[56] IBM estimated that addressing the issues would cost $180 million. In October 2009, the state announced it had canceled the deal because IBM failed to make the proposed improvements to the satisfaction of the state.[57]

In May 2010, the state of Indiana sued IBM for $1.3 billion, claiming breach of contract. The Indiana FSSA claimed that system-processing errors resulted in incorrect denials of benefits

and delays in processing claims bringing harm to in-need citizens. The claims mishandling rate had climbed from 4 percent to 18 percent under the new system.[58] FSSA spokesman Marcus Barlow stated that "there was more staff working on eligibility during IBM's tenure than before IBM came, yet the results show that once IBM put their system in place, timeliness got worse, error rates went higher. Backlogs got larger."[59]

When the FSSA defined the project in 2006, they told IBM that, for staffing flexibility and efficiency, they wanted a system that would not assign one citizen to a single caseworker. Thus, IBM designed a task-based process that involved outsourcing 1,500 former FSSA employees to IBM. These workers interacted with welfare applicants to gather the necessary data to apply for welfare. Once these workers completed their tasks, the application was turned over to some 700 FSSA state workers who used the accumulated data to determine benefits eligibility.[60]

An IBM spokesman asserted that while there were delays in the system, it was because there were an insufficient number of workers to handle the number of claims. In addition, IBM pointed out that during contract negotiations with IBM, FSSA specified that the system be able to handle up to 4,200 applications per month. However, during the severe recession of 2008–2010, the number of applications frequently exceeded 10,000 per month.[61] The IBM spokesman made it clear that changing from the assigned caseworker approach was Indiana's idea, and was not proposed by IBM.[62] FSSA has since implemented a hybrid system that incorporates the "successful elements of the old welfare delivery system" and a "modernized system." This system assigns caseworkers to welfare recipients and allows for more face-to-face contact.

In its lawsuit, Indiana is demanding that IBM refund the $437 million the state already paid to IBM. Indiana also wants reimbursement of all overtime pay state employees earned working longer hours due to problems with the system. In addition, Indiana insists that IBM be liable for any federal penalties or damages from any lawsuits filed by others because of delays in payments to citizens. IBM countersued Indiana to keep the $400 million it was already paid and for an additional $53 million for the equipment it left in place, which FSSA workers are now using.[63]

In a press release issued at the time the lawsuit was filed, IBM claimed that Indiana had acknowledged that the new system had reduced fraud that was estimated to cost over $100 million per year, led to creation of 1,000 new jobs, and reduced Indiana's operating expenses by $40 million per year for 2008 and 2009 with projected savings of hundreds of millions in upcoming years.[64]

In a 2012 court ruling, the judge ruled that IBM is not entitled to the more than $400 million it sought from Indiana. In the same ruling, the judge denied IBM's claim for damages, while ordering Indiana to pay $12 million for equipment provided by IBM.[65]

Discussion Questions

1. Experienced observers point out that the development of a state social services system is always exceedingly difficult. Multiagency interaction and interdependence often leads to delays and complications in getting requirements finalized and agreed upon. And even if that is accomplished, changes in welfare policies by the state or federal government can render those requirements invalid and require considerable rework. Given the problems that IBM encountered on this contract, should it decline the future opportunities it may have to propose a new solution for a state social services system?

2. Present a strong argument that the state of Indiana is entitled to reimbursement of all funds paid to IBM as well as reimbursement of all overtime employees were paid due to fixing problems associated with the new system. Now present a strong argument that IBM should be allowed to keep all funds it has received so far for this new system.
3. Read about the judge's recent ruling in this case (*www.govtech.com/health/Nobody-Wins-in-Indiana-vs-IBM-Lawsuit-Judge-Says.html*). Do you agree or disagree with the ruling? Provide three reasons to support your opinion.

3. When Certification Is Justified

When Don Tennant, former editor-in-chief of *Computerworld*, published an editorial in favor of IT certification, he was promptly hit with a barrage of angry responses from IT workers.[66] They argued that testable IT knowledge does not necessarily translate into quality IT work. A worker needs good communication and problem-solving skills as well as perseverance to get the job done well. Respondents explained that hardworking IT workers focus on skills and knowledge that are related to their current projects and don't have time for certifications that will quickly become obsolete. Many readers indicated they suspected that vendors offer certification simply as a marketing ploy and a source of revenue. They accused managers without technical backgrounds of using certification as "a crutch, a poor but politically defensible substitute for knowing what and how well one's subordinates are doing."[67]

Any manager would certainly do well to review these insightful points, yet they beg the question: What useful purposes *can* certification serve within an organization?

Some CIOs and vice presidents of technology assert that many employers use certification as a means of training employees and increasing skill levels within the company. Some companies are even using certification as a perk to attract and keep good employees. Such companies may also enhance their employee training programs by offering a job-rotation program through which workers can acquire certification and experience.

Employers are also making good use of certification as a hiring gate both for entry-level positions and for jobs that require specific core knowledge. For example, a company with a Windows Server network might run an ad for a systems integration engineer and require a Microsoft Certified Systems Engineer (MCSE) certification. A company that uses Siebel customer relationship management software might require a new hire to have a certification in the latest version of Siebel.

In addition, specific IT fields, such as project management and security, have a greater need for certification. As the speed and complexity of production increase within the global marketplace, workers in a variety of industries are showing an increasing interest in project management certification. With mottos like "Do It, Do It Right, Do It Right Now," the Project Management Institute has already certified more than 400,000 people. IT industry employers are beginning to encourage and sometimes require project management certification.

Calls for training in the field of security management go beyond certification. The demand for security workers is expected to continue to grow rapidly in the next few years in the face of growing threats. Spam, computer viruses, spyware, botnets, and identity theft have businesses and government organizations worried. They want to make sure that their security managers can protect their data, systems, and resources.

One of the best-recognized security certifications is the CISSP, awarded by the International Information Systems Security Certification Consortium. Yet the CISSP examination, like so many other IT certification examinations, is multiple choice. Employers and IT workers alike have begun to recognize the limitations of these types of examinations. They want to ensure that examinees not only have core knowledge but also know how to use that knowledge—and a multiple-choice exam, even a six-hour, 250-question exam like the CISSP, can't provide that assurance.

Other organizations are catching on. Sun Microsystems requires the completion of programming or design assignments for some of its certifications. So, while there is no universal call for certification or a uniform examination procedure that answers all needs within the IT profession, certifying bodies are beginning to adapt their programs to better fulfill the evolving needs for certification in IT.

Discussion Questions

1. How can organizations and vendors change their certification programs to test for skills as well as core knowledge? What issues might this introduce?
2. What are the primary arguments against certification, and how can certifying bodies change their programs to overcome these shortcomings?
3. What are the benefits of certification? How might certification programs need to change in the future to better serve the needs of the IT community?

End Notes

[1] "CityTime," *New York Times*, March 14, 2012, http://topics.nytimes.com/top/reference/timestopics/organizations/o/office_of_payroll_administration_nyc/citytime/index.html.

[2] "CityTime," *New York Times*, March 14, 2012, http://topics.nytimes.com/top/reference/timestopics/organizations/o/office_of_payroll_administration_nyc/citytime/index.html.

[3] "CityTime," *New York Times*, March 14, 2012, http://topics.nytimes.com/top/reference/timestopics/organizations/o/office_of_payroll_administration_nyc/citytime/index.html.

[4] "CityTime," *New York Times*, March 14, 2012, http://topics.nytimes.com/top/reference/timestopics/organizations/o/office_of_payroll_administration_nyc/citytime/index.html.

[5] Ali Winston, "Comptroller Moves to Rein in CityTime," *CityLimits*, February 26, 2012, www.citylimits.org/news/articles/3896/comptroller-moves.

[6] Serge F. Kovaleski and John Eligon, "New York City Payroll Chief Resigns," *New York Times*, December 23, 2010, www.nytimes.com/2010/12/24/nyregion/24citytime.html.

[7] Serge F. Kovaleski and John Eligon, "New York City Payroll Chief Resigns," *New York Times*, December 23, 2010, www.nytimes.com/2010/12/24/nyregion/24citytime.html.

[8] David W. Chen and William K. Rashbaum, "With Arrest, Criticism for Payroll Project Grows," *New York Times*, May 27, 2011, www.nytimes.com/2011/05/28/nyregion/criticism-for-citytime-project-grows-as-a-manager-is-arrested.html.

[9] Colin Moynihan, "Early Trial Planned for Defendants in CityTime Case," *New York Times*, March 15, 2012, http://cityroom.blogs.nytimes.com/2012/03/15/early-2013-trial-planned-for-defendants-in-citytime-case.

[10] "CityTime," *New York Times*, March 14, 2012, http://topics.nytimes.com/top/reference/timestopics/organizations/o/office_of_payroll_administration_nyc/citytime/index.html.

[11] U.S. Code, Title 5, Part III, Subpart F, Chapter 71, Subchapter 1, Section 7103, http://law.justia.com/us/codes/title5/5usc7103.html (accessed December 27, 2012).

[12] BSA | The Software Alliance, "Record Period of Settlements Underscores Persistent Software Piracy Problem in the US," August 21, 2012, www.bsa.org/country/News%20and%20Events/News%20Archives/en/2012/en-08212012-US.aspx.

[13] BSA | The Software Alliance, "Tennessee Automotive Dealer Pays Heavy Fines," March 7, 2012, www.bsa.org/country/News%20and%20Events/News%20Archives/en/2012/en-03072012-TN.aspx.

[14] Anthony Ha, "Zynga Falls Short of Analysts Estimate for Q2: $332 Million in Revenue, Bookings Decline From Last Quarter, Lowered Outlook," *Tech Crunch*, July 25, 2012, http://techcrunch.com/2012/07/25/zynga-earnings-q2.

[15] Tricia Duryee, "Zynga Files Suit Against Former Staffer, Claiming Theft of Trade Secrets," *AllThingsD.com,* October 14, 2012, http://allthingsd.com/20121014/zynga-files-suit-against-former-staffer-claiming-theft-of-trade-secrets.

[16] Paul McDougall, "Indian Outsourcer Infosys Eyed for Visa Fraud," *InformationWeek*, August 18, 2011, www.informationweek.com/services/outsourcing/indian-outsourcer-infosys-eyed-for-visa/231500239.

[17] Paul McDougall, "Infosys Wins Court Battle, But Visa Troubles Continue," *InformationWeek*, August 21, 2012, www.informationweek.com/global-cio/outsourcing/infosys-wins-court-battle-but-visa-troub/240005939.

[18] Steven Musil, "Man Suing for Half of Facebook Loses Lawyer," *CNET*, June 28, 2011, http://news.cnet.com/8301-1023_3-20075244-93/man-suing-for-half-of-facebook-loses-lawyer.

[19] Thomas Claburn, "Ceglia To Face Facebook Fraud Charges," *InformationWeek*, October 27, 2012, www.informationweek.com/internet/social-network/ceglia-to-face-facebook-fraud-charges/240010623.

[20] "Misleading and Deceptive: Apple Sued Over Siri," *Sydney Morning Herald*, March 14, 2012, www.smh.com.au/digital-life/mobiles/misleading-and-deceptive-apple-sued-over-siri-20120314-1uz3d.html.

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

[22] Eli Segall, "Oracle to Pay $200M in Settlement," *Silicon Valley/San Jose Business Journal*, October 6, 2011, www.bizjournals.com/sanjose/news/2011/10/06/oracle-to-pay-200m-in-settlement.html?page=all.

[23] Paul McDougall, "Ex-Apple Manager Guilty In Kickback Scheme," *InformationWeek*, March 1, 2011, www.informationweek.com/hardware/apple-macintosh/ex-apple-manager-guilty-in-kickback-sche/229219586.

[24] United States Department of Justice, "Foreign Corrupt Practices Act: Antibribery Provisions," www.justice.gov/criminal/fraud/fcpa/docs/lay-persons-guide.pdf (accessed November 9, 2012).

[25] "G20 Throws Weight Behind Global Anti-Corruption Treaty," *TrustLaw*, November 12, 2010, www.trust.org/trustlaw/news/g20-throws-weight-behind-global-anti-corruption-treaty.

[26] Stu Woo, "New Chief Brings Affable Manner and A Boston Accent," *Wall Street Journal*, January 5, 2012, http://online.wsj.com/article/SB10001424052970203513604577140762129761548.html.

[27] Julianne Pepitone, "Yahoo Confirms CEO Is Out After Resume Scandal," *CNN Money*, May 14, 2002, http://money.cnn.com/2012/05/13/technology/yahoo-ceo-out/index.htm.

[28] Ropella, "Hiring Smart: How to Avoid the Top Ten Mistakes," www.ropella.com/index.php/knowledge/recruitingProcessArticles/hiring_smart, © 2012 Ropella Group Inc.

[29] Leo Ma, "Resume Exaggeration in Asia Pacific," *Ezine Articles*, http://ezinearticles.com/?Resume-Exaggeration-in-Asia-Pacific&id=4788569, August 6, 2010.

[30] Association for Computing Machinery, "Welcome," www.acm.org (accessed November 11, 2012).

[31] IEEE Computer Society, "About Us—About the Computer Society," www.computer.org/portal/web/about (accessed November 11, 2012).

[32] IEEE Computer Society, "Computer Society and ACM Approve Software Engineering Code of Ethics," *Computer Society Connection*, October 1999, www.computer.org/cms/Computer.org/Publications/code-of-ethics.pdf (accessed December 28, 2012).

[33] Association of Information Technology Professionals, "About AITP: History," www.aitp.org/organization/about/history/history.jsp (accessed November 11, 2012).

[34] SysAdmin, Audit, Network, Security (SANS) Institute, "Information Security Training, Certification & Research," www.sans.org/about/sans.php (accessed November 11, 2012).

[35] John Cox, "Android Software Piracy Rampant Despite Google's Efforts to Curb," *Network World*, September 29, 2010, www.networkworld.com/news/2010/092910-google-android-piracy.html.

[36] Andres Millington, "Porn in the Workplace is Now a Major Board-Level Concern for Business," *Business Computing World*, April 23, 2010, www.businesscomputingworld.co.uk/porn-in-the-workplace-is-now-a-major-board-level-concern-for-business.

[37] Dean Wilson, "Third of Mobile Workers Distracted by Porn, Report Finds," *TechEYE.net*, June 14, 2010, www.techeye.net/mobile/third-of-mobile-workers-distracted-by-porn-report-finds.

[38] Tony Capaccio, "Missile Defense Staff Warned to Stop Surfing Porn Sites," *Bloomberg*, August 2, 2012, www.bloomberg.com/news/2012-08-01/missile-defense-staff-warned-to-stop-surfing-porn-sites.html.

[39] Associated Press, "WikiLeaks Reveals Sensitive Diplomacy," *Cincinnati Enquirer*, November 28, 2010.

[40] Matthew J. Schwartz, "California Targets Mobile Apps for Missing Privacy Policies," *InformationWeek*, October 31, 2012, www.informationweek.com/government/mobile/california-targets-mobile-apps-for-missi/240012603.

[41] Annemarie K. Keinath and Judith C. Walo, "Audit Committees Responsibilities," *The CPA Journal Online*, www.nysscpa.org/cpajournal/2004/1104/essentials/p22.htm (accessed November 11, 2012).

[42] Shareholders Foundation, Inc. "Press Release: Sensata Technologies Holding N.V. Under Investor Investigation Over Possible Foreign Bribery," *PRLog*, October 26, 2010, www.prlog.org/11024869-sensata-technologies-holding-nv-under-investor-investigation-over-possible-foreign-bribery.html.

[43] SuccessFactors, "SuccessFactors 2010 Annual Report," http://phx.corporate-ir.net/phoenix.zhtml?c=214238&p=irol-reportsAnnual (accessed January 13, 2013).

[44] SuccessFactors, "SuccessFactors 2011 Annual Report," www.sap.com/corporate-en/investors/reports/pdf/SFSF-2011-Annual-Report.pdf (accessed January 13, 2013).

[45] The Linesch Firm, "Whistleblower Sheds Light on Fraud," November 2, 2012, http://lineschfirm.com/wp/whistleblower-sheds-light-on-fraud.

[46] Larry Dignan, "SAP Acquires SuccessFactors for $3.4 Billion: Cloud Consolidation Accelerates," *ZDNet*, December 3, 2011, www.zdnet.com/blog/btl/sap-acquires-successfactors-for-3-4-billion-cloud-consolidation-accelerates/64627.

[47] "Press Release: SuccessFactors Announces Preliminary Fourth Quarter Fiscal 2011 Results," *PRNewswire*, February 2, 2012, www.bizjournals.com/prnewswire/press_releases/2012/02/02/SF46931.

[48] SuccessFactors, "Annual Report 2008," http://media.corporate-ir.net/media_files/irol/21/214238/LetterAnnual08.pdf (accessed January 28, 2013).

[49] SuccessFactors, "Annual Report 2008," http://media.corporate-ir.net/media_files/irol/21/214238/LetterAnnual08.pdf (accessed January 28, 2013).

[50] Scott Priest, "Today in SAP: Allegations Build Over SuccessFactors' Accounting," *SAPexperts*, October 26, 2012, http://sapexperts.wispubs.com/IT/IT-Blog/2012/October/Today-in-SAP-10262012.

[51] Francine McKenna, "Is the SEC's Ponzi Crusade Enabling Companies to Cook the Books, Enron-Style?," *Forbes*, October 18, 2012, www.forbes.com/sites/francinemckenna/2012/10/18/is-the-secs-ponzi-crusade-enabling-companies-to-cook-the-books-enron-style.

[52] Julia Bort, "Whistleblower Explains One Way Cloud Companies Can Cook Their Books," *BusinessInsider,* October 25, 2012, www.businessinsider.com/successfactors-accounting-whistleblower-speaks-2012-10.

[53] Francine McKenna, "Is the SEC's Ponzi Crusade Enabling Companies to Cook the Books, Enron-Style?," *Forbes*, October 18, 2012.

[54] "IBM Closes In on $1.16bn Indiana Deal," *Computer Business Review*, November 29, 2006, www.cbronline.com/news/ibm_closes_in_on_116bn_indiana_deal (accessed November 12, 2010).

[55] Associated Press, "Indiana: IBM Welfare Intake Work Flawed from Start," *Indianapolis Business Journal*, July 21, 2010, www.ibj.com/indiana-ibm-welfare-intake-work-flawed-from-start/PARAMS/article/21227.

[56] Ken Kusmer, Associated Press, "IBM on Notice over Indiana Welfare Deal, *FortWayne.com*, www.newssentinel.com/apps/pbcs.dll/article?AID=/20090708/NEWS/907080335 (accessed December 19, 2010).

[57] Audrey B., "IBM vs. Indiana: Big Blue Makes Indiana See Red," *Seeking Alpha* (blog), May 18, 2010, http://seekingalpha.com/article/205668-ibm-vs-indiana-big-blue-makes-indiana-see-red.

[58] Robert Charette, "Indiana and IBM Sue Each Other Over Failed Outsourcing Contract," *IEEE Spectrum Risk Factor* (blog), May 14, 2010, http://spectrum.ieee.org/riskfactor/computing/it/indiana-and-ibm-sue-each-other-over-failed-outsourcing-contract.

[59] Andy Opsahl, "IBM and Indiana Suing Each Other Over Canceled Outsourcing Deal," *Government Technology*, May 13, 2010, www.govtech.com/health/IBM-and-Indiana-Suing-Each-Other.html.

[60] Andy Opsahl, "IBM and Indiana Suing Each Other Over Canceled Outsourcing Deal," *Government Technology*, May 13, 2010, www.govtech.com/health/IBM-and-Indiana-Suing-Each-Other.html.

[61] Andy Opsahl, "IBM and Indiana Suing Each Other Over Canceled Outsourcing Deal," *Government Technology*, May 13, 2010, www.govtech.com/health/IBM-and-Indiana-Suing-Each-Other.html.

[62] Andy Opsahl, "IBM and Indiana Suing Each Other Over Canceled Outsourcing Deal," *Government Technology*, May 13, 2010, www.govtech.com/health/IBM-and-Indiana-Suing-Each-Other.html.

[63] Andy Opsahl, "IBM and Indiana Suing Each Other Over Cancelled Outsourcing Deal," *Government Technology*, May 13, 2010, www.govtech.com/health/IBM-and-Indiana-Suing-Each-Other.html.

[64] IBM, "Press Release: IBM Seeks Enforcement of Indiana Welfare Contract," May 13, 2010, www-03.ibm.com/press/us/en/pressrelease/31641.wss.

[65] Colin Wood, "Nobody Wins in Indiana vs. IBM Lawsuit, Judge Says," *Government Technology*, July 19, 2012, www.govtech.com/health/Nobody-Wins-in-Indiana-vs-IBM-Lawsuit-Judge-Says.html.

[66] Don Tennant, "Certifiably Concerned," *Computerworld*, June 13, 2005, www.computerworld.com/s/article/102394/Certifiably_Concerned.

[67] Don Tennant, "Certifiably Mad?," *Computerworld*, June 20, 2005, www.computerworld.com/s/article/102564/Certifiably_Mad.

CHAPTER 3

COMPUTER AND INTERNET CRIME

QUOTE

The most dangerous criminal may be the man gifted with reason, but with no morals.
—Martin Luther King, Jr.

VIGNETTE

The Reveton Ransomware Attacks

In August 2012, the Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center, was inundated with reports of a new type of cybercrime. Victims across the United States reported that while searching the Internet, their computers locked up, and they received the following message, purportedly from the FBI: "This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)" The message then accused the victim either of visiting pornography Web sites or of distributing copyrighted content. Victims were told they could unlock their computers and avoid prosecution by paying a fine of $200 within 72 hours of receiving the message. The message came replete with the official FBI logo.[1]

The incident pointed to a steep rise in ransomware attacks. **Ransomware** is malware that disables a computer or smartphone until the victim pays a fee, or ransom. Unlike other viruses, the

Reveton version of ransomware is not activated by opening a file or an attachment. Rather it is an example of "drive-by malware," viruses that download automatically when a user visits an infected Web site.[2]

The FBI immediately issued an alert, but within a month, cybersecurity experts had identified 16 variants of the ransomware. These viruses had infected 68,000 unique IP addresses. It is estimated that on an average day, about 170 victims paid the $200 fee and received valid unlock codes.[3] The compromised computers could not be fixed through the installation or updating of antivirus software because the computer was locked. Because so many home PC owners fail to back up their systems regularly, many victims faced losing a significant amount of data. The $200 fee itself was low enough to encourage payment. A visit to a professional IT service to repair the damage could potentially cost the same amount and take more time to resolve. A quick payment through a prepaid money card system, such as MoneyPak, could save the victim a lot of trouble.

The United States was not the first country to be hit by these attacks. In early 2012, criminal gangs targeted France, Germany, and the United Kingdom. Ransomware attacks first broke out in Russia in 2009. Since that time, they have spread to almost every country on the globe, hitting the United States and Japan especially hard. Symantec, an IT security company, estimates that gangs are extorting over $5 million per year from online victims.[4] The rise of ransomware attacks is, no doubt, due in part to their success. In France, for example, almost 4 percent of victims coughed up the ransom money during a non-Reveton scam.[5]

The Reveton ransomware is delivered by the popular Russian-language Citadel malware toolkit. The latest version of Citadel can also grab passwords from Web browsers and change Web sites to trick users into handing over their login information.[6]

In December 2012, the United Kingdom arrested three people they believed were involved in the Reveton ransomware attacks.[7] Finding the perpetrators, however, is unusual and is not the most effective way to combat this crime. Law enforcement agencies and IT security companies have urged the public to take measures to prevent themselves from falling victim to such attacks—by keeping software such as Java, Acrobat Reader, Adobe Flash, Windows, and their browser software updated. An early Reveton ransomware attack made use of a vulnerability in a version of Java that had just been patched a month prior.[8] Computer users can also avoid infections by using security software that identifies suspicious Web sites, and by not clicking online ads from dubious companies.[9] Perhaps, however, the best way to avoid the spread of these attacks is to encourage victims to report the crime and to refuse to comply with the ransom demands.

Questions to Consider

1. Why are ransomware attacks on the rise?
2. What can you do to prevent ransomware attacks on your own computer?
3. How do you think victims should respond to ransomware attacks? Do they have an ethical obligation to future victims?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What key trade-offs and ethical issues are associated with the safeguarding of data and information systems?
2. Why has there been a dramatic increase in the number of computer-related security incidents in recent years?
3. What are the most common types of computer security attacks?
4. Who are the primary perpetrators of computer crime, and what are their objectives?
5. What are the key elements of a multilayer process for managing security vulnerabilities based on the concept of reasonable assurance?
6. What actions must be taken in response to a security incident?
7. What is computer forensics, and what role does it play in responding to a computer incident?

IT SECURITY INCIDENTS: A MAJOR CONCERN

The security of information technology 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 necessity of security is obvious, it must often be balanced against other business needs. Business managers, IT professionals, and IT users all face a number of ethical decisions regarding IT security, such as the following:

- If a firm is a victim of a computer crime, should it pursue prosecution of the criminals at all costs, maintain a low profile to avoid the negative publicity, inform its affected customers, or take some other action?
- How much effort and money should be spent to safeguard against computer crime? (In other words, how safe is safe enough?)
- If a company realizes that it has produced software with defects that make it possible for hackers to attack customer data and computers, what actions should it take?
- 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?

Table 3-1 shows the occurrence of common computer security incidents at 149 U.S.-based organizations that responded to the 2010/2011 CSI Computer Crime and Security Survey.

TABLE 3-1 Most common computer-related security incidents

	Percent of organizations that experienced this type of incident		
Type of incident	**2008**	**2009**	**2010**
Malware infection	50%	64%	67%
Being fraudulently represented as the sender of email messages requesting personal information	31%	34%	39%
Laptop or mobile hardware loss	42%	42%	34%
Employee abuse of Internet access or email (e.g., accessing pornography or use of pirated software)	44%	30%	25%

Source Line: "2010/11 Computer Security Institute Computer Crime & Security Survey," courtesy of the Computer Security Institute.

Why Computer Incidents Are So Prevalent

In today's computing environment of increasing complexity, higher user expectations, expanding and changing systems, and growing reliance on software with known vulnerabilities, it is no wonder that the number, variety, and impact of security incidents are increasing dramatically. Computer security incidents occur around the world with personal computer users in developing countries being exposed to the greatest risk of

their computers being infected by malware. Table 3-2 shows the ranking of the best and worst countries in terms of percent of computers infected by malware as determined by Kaspersky Lab, a provider of computer security software and services.

TABLE 3-2 Country ranking based on percent of infected computers

Countries with highest rate of infected computers		Countries with lowest rate of infected computers	
Country	**Rate**	**Country**	**Rate**
Sudan	70%	Japan	6%
Bangladesh	64%	Germany	9%
Iraq	62%	Switzerland	10%
Rwanda	57%	Luxembourg	10%
Nepal	56%	Denmark	11%

Source Line: Stefan Tanase, "Q1/2011 Malware Report," Kaspersky Lab, May 17, 2011.

Separately, the Business Software Alliance recently analyzed 24 countries representing the major users of information and communications technology in the world. The countries were rated based on data privacy, cybersecurity, cybercrime control, protection of intellectual property, IT infrastructure, free trade, technology interoperability, and the compatibility of country criminal laws with international standards regarding computer crime. Japan was the highest ranked country—with Australia, Germany, the United States, and France also rated highly. Brazil was rated dead last, primarily because it has no law that guarantees the privacy of data transfer, and its laws against cybercrime are very weak. It is estimated that in 2011, computer hackers stole over $1 billion (USD) from businesses in Brazil—32 percent of Brazilian businesses were victims of cyberattacks.[10]

Increasing Complexity Increases Vulnerability

The computing environment has become enormously complex. Networks, computers, operating systems, applications, Web sites, 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.

To further complicate matters, workers in many organizations operate in a **cloud computing** environment in which software and data storage are services provided via the Internet ("the cloud"); the services are run on another organization's computer hardware and are accessed via a Web browser. This represents a significant change in how data is stored, accessed, and transferred, and it raises many security concerns. The unmanaged employee use of cloud services (e.g., the use of a file-sharing Web site to transfer large documents to clients or suppliers) represents a significant risk. IT and business managers should insist that employees choose from a list of validated cloud services to avoid potential issues. Table 3-3 provides some key questions to ask when evaluating cloud services. The preferred answer to each question is *yes*.

TABLE 3-3 Questions to ask when evaluating cloud services

Question	Yes	No
Are the interfaces between the cloud service and users secure, with appropriate levels of access control?		
Is data encrypted as it travels over the Internet?		
Does the service provide secure storage and access control over data stored in the cloud?		
Does the service provide backup capabilities in the event that a human-caused or natural disaster renders the primary service unusable?		
Is the cloud service provider reputable and financially viable?		

Source Line: Course Technology/Cengage Learning.

Virtualization also introduces further complications into today's computer environment. **Virtualization software** operates in a software layer that runs on top of the operating system. It enables multiple virtual machines—each with their own operating system—to run on a single computer. Each of these **virtual machines** performs as if it is a separate computer, completing required tasks for the users and applications assigned to that virtual machine. Virtualization takes advantage of the fact that most physical servers utilize less than 10 percent of their hardware capacity. With virtualization, the workload from multiple physical servers can be handled by separate virtual machines on a single physical server. Virtualization thus increases resource sharing and system utilization, greatly reducing the number of servers required to handle an organization's processing needs. Fewer servers mean less computing space and less power is required to operate and cool the servers. Thus, virtualization lowers costs and reduces space requirements.[11] However, operating in a virtual environment greatly complicates the operating environment and raises the potential harm if a single virtualized server is compromised by a hacker.

Higher Computer User Expectations

Today, time means money, and the faster computer users can solve a problem, the sooner they can be productive. As a result, computer help desks are under intense pressure to respond very quickly to users' questions. Under duress, help desk personnel sometimes forget to verify users' identities or to check whether they are authorized to perform a requested action. In addition, even though most have been warned against doing so, some computer users share their login ID and password with other coworkers who have forgotten their own passwords. This can enable workers to gain access to information systems and data for which they are not authorized.

Expanding and Changing Systems Introduce New Risks

Business has moved from an era of stand-alone computers, in which critical data was stored on an isolated mainframe computer in a locked room, to an era in which personal

computers 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 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.

Bring Your Own Device

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 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 simply 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 Web sites, blogging, shopping, visiting social networks, and so on) 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, BYOD makes it extremely difficult for IT organizations to adequately safeguard additional portable devices with various operating systems and a myriad of applications.

Increased 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. (These fixes are in addition to other maintenance and project work that software developers perform.) For example, a critical vulnerability was discovered in Oracle's Java 7 software that made it possible for a hacker to break into computers. Oracle released an emergency software fix to correct this problem.[12]

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 an ethical 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? Since 2006, the number of new software vulnerabilities identified has been in excess of 4,600 per year (an average of 13 per day), as shown in Table 3-4.

TABLE 3-4 Total number of new software vulnerabilities identified annually

Year	Number of software vulnerabilities identified
2006	4,842
2007	4,644
2008	5,562
2009	4,814
2010	6,253
2011	4,989

Source Line: "Internet Security Threat Report: 2011 Trends," Symantec, April 2012, www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf.

Clearly, it can be difficult to keep up with all the required patches. Of special concern is a **zero-day attack** that takes place before the security community or software developer knows about the vulnerability or has been able to repair it. One would hope that the discoverer of a zero-day vulnerability would provide his knowledge to the original software manufacturer so that a fix can be created for the problem. However, in some cases, this knowledge is sold on the black market to cyberterrorists, governments, or large organizations that may then use it themselves in attacks on the computers of a rival. Zero-day exploits can command prices as high as $250,000.[13]

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 suggested by current users or potential customers that will help sell the software.

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 the virus, worm, Trojan horse, spam, distributed denial-of-service, rootkit, phishing, spear-phishing, smishing, and vishing.

While we usually think of such exploits being aimed at computers, smartphones such as Apple's iPhone, Research In Motion's BlackBerry, and numerous smartphones based on Google's Android operating system 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 a target for cyberthieves. As discussed in the opening vignette, ransomware is a form of malware, which when downloaded onto a smartphone, takes control of the device and its data until the owner agrees to pay a ransom to the attacker.[14] Another form of smartphone malware runs up charges on users' accounts by automatically sending messages to numbers that charge fees upon receipt of a message.[15]

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. Often a virus is attached to a file, so that when the infected file is opened, the virus executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies, or creates them. Most viruses deliver a "payload," or malicious software that causes the computer to perform in an unexpected way. For example, the virus may be programmed to display a certain message on the computer's display screen, delete or modify a certain document, or reformat the hard drive.

A true virus does not spread itself from computer to computer. A virus is spread to other machines when a computer user opens an infected email attachment, downloads an infected program, or visits infected Web sites. In other words, viruses 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 email with the subject line "Resume - Janet Simons." If the email recipient clicks on the attachment, the virus deletes all data in the recipient's mapped drives.

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.

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.[16,17]

Trojan Horses

A **Trojan horse** is a program in which malicious code is hidden inside a seemingly harmless program. 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 Social Security numbers, or spy on users by recording keystrokes and transmitting them to a server operated by a third party.

A Trojan horse can be delivered as an email attachment, downloaded from a Web site, or contracted via a removable media device such as a CD/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.

Win-7 Anti-Virus 2012 is a fake antivirus tool that infiltrates users' computers through the use of a Trojan horse. Once on a user's computer, the fake tool simulates a system scan and purports to find numerous infections of malware. It claims it can remove these infections if you purchase the tool by providing your credit card information.[18]

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 by a specific time or date.

Spam

Email **spam** is the abuse 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 method of marketing 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. Spam is also used to deliver harmful worms and other malware.

The cost of creating an email campaign for a product or service is several hundred to a few thousand dollars, compared with tens of thousands of dollars for direct-mail campaigns. In addition, email campaigns take only a couple of weeks 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 can 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 users time to scan and delete spam email, a cost that can add up if they pay for Internet connection charges on an hourly basis. 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.

The **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act** went into effect in January 2004. The act says 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 68 percent in October 2012, according to Securelist, a blog run by the computer security firm Kaspersky Labs.[19]

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 but all but the most sophisticated computer programs cannot. For example, humans can read the distorted text in Figure 3-1, but simple computer programs cannot.

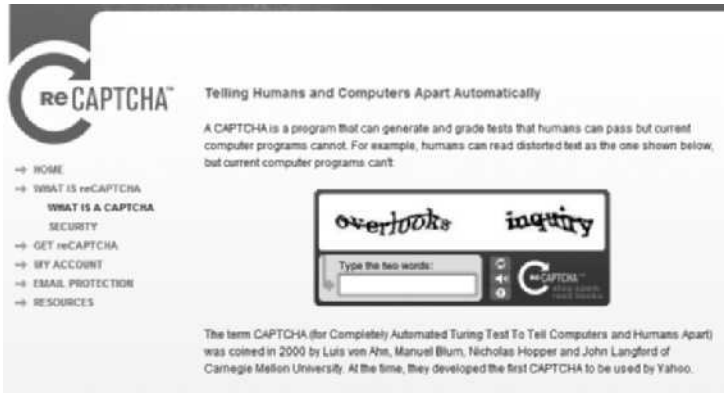


FIGURE 3-1 Example of CAPTCHA
Source Line: CAPTCHA example from www.recaptcha.net. Courtesy of Carnegie Mellon University.

Distributed Denial-of-Service (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 distributed denial-of-service 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 "holds the line open" while waiting for a reply that never comes, and eventually the requests exhaust all resources of the target, as illustrated in Figure 3-2.

The software to initiate a denial-of-service attack is simple to use, and over 55 DDoS tools are readily available at a variety of hacker sites.[20] 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 are so overwhelmed by requests for service that legitimate users are unable to "get through" to the target computer. Banks and other e-commerce Web sites are frequent targets of botnets. Both the Bank of America and Chase banks were hit with a DDoS attack in the fall of 2012.[21]

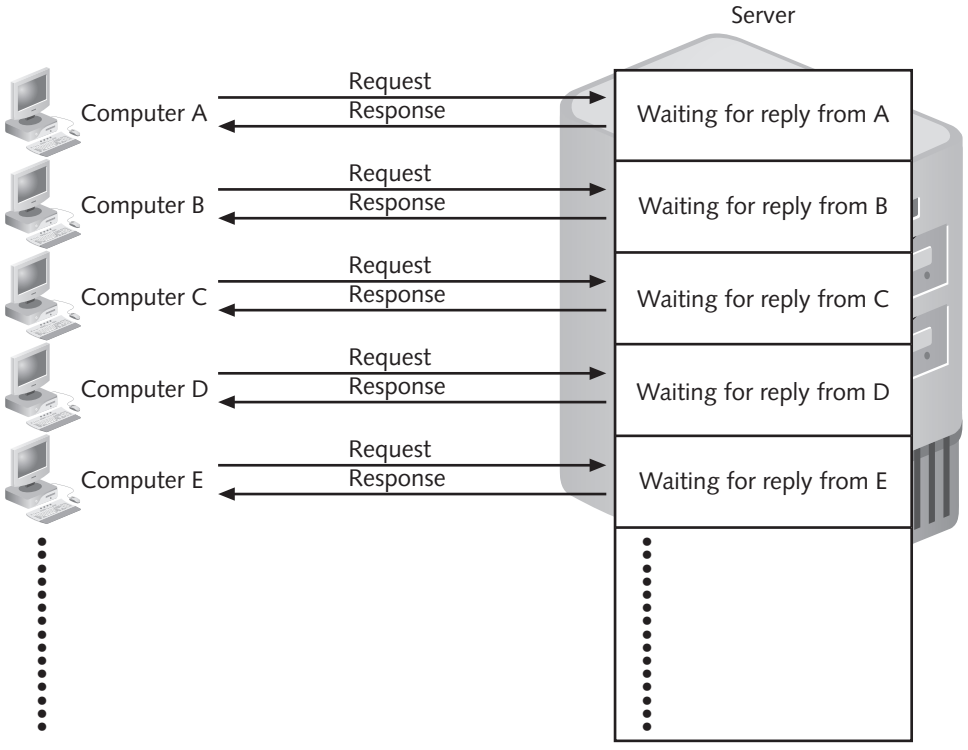


FIGURE 3-2 Distributed denial-of-service attack
Source Line: Course Technology/Cengage Learning.

Botnets are also frequently used to distribute spam and malicious code. The Grum botnet was first detected in 2008 and operated until 2012 when it was brought down by cybercrime fighters. Grum infected several hundred thousand computers around the world. It generated prodigious amounts of spam advertising cheap pharmaceutical products. At its peak, Grum is estimated to have been responsible for 35 percent of the world's spam.[22]

Rootkits

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 blended threat, consisting of the dropper, loader, and rootkit. The dropper code gets the rootkit installation started and can be activated by clicking on a link to a malicious Web site 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 currently running cannot be trusted to provide valid test results. Here 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.

A recent rootkit, labeled 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.[23]

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 Web site or opening an email attachment. These emails, such as the one shown in Figure 3-3, lead consumers to counterfeit Web sites designed to trick them into divulging personal data.


EBAY INC: PLEASE CONFIRM YOUR BANKING DETAILS - Message (HTML)

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 phishing
Source Line: Course Technology/Cengage Learning.

Savvy users often become suspicious and refuse to enter data into the fake Web sites; however, sometimes just accessing the Web site can trigger an automatic and unnoticeable download of malicious software to a computer. Citibank, eBay, and PayPal are among the Web sites that phishers spoof most frequently. It is estimated that .03 percent of all emails sent in October 2012 were phishing attacks.[24]

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 Web site 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.

Strategic Forecasting (commonly referred to as Stratfor) is an intelligence analysis firm whose clients include the U.S. Army, the Department of Defense, and military contractor Lockheed Martin. A hacker group broke into the firm's network and stole information on thousands of email accounts. This information was used to initiate spear-phishing attacks on employees of the firm's clients. The emails, which were designed to look as if they came from Stratfor, directed recipients to a Web site that looked like the Stratfor Web site and instructed them to enter private information. In addition, the emails were laced with malware and other harmful attachments.[25]

Smishing and Vishing

Smishing is another variation of phishing that involves the use of Short Message Service (SMS) texting. In a smishing scam, people receive a legitimate-looking text message on their phone telling them to call a specific phone number or to log on to a Web site. This is often done under the guise that there is a problem with their bank account or credit card that requires immediate attention. However, the phone number or Web site 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. This information can 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 Web site, malicious software is downloaded onto their phones, providing criminals with access to information stored on the phones. The number of smishing scams increases around the holidays as people use their cell phones to make online purchases. **Vishing** is similar to smishing except that the victims receive a voice mail telling them to call a phone number or access a Web site. Here are two examples of smishing crimes:

- Account holders at a credit union were sent a text about an account problem and were told to call a phone number provided in the text. If they did so, they were asked to provide personal information that allowed criminals to steal funds from their accounts within 10 minutes of the phone call.
- Bank customers received a text stating that it was necessary to reactivate their automated teller machine (ATM) card. Those who called the phone number in the text were asked to provide their ATM card number, PIN, and expiration date. Thousands of victims had money stolen from their accounts.[26]

Financial institutions, credit card companies, and other organizations whose customers may be targeted by criminals in this manner need to 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 Web site.
- 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 Federal Bureau of Investigation (FBI).
- Institutions can also try to notify the telecommunications carrier for the particular phone number that victims are requested to call, to request that they shut down that number.[27]

Types of Perpetrators

The people who launch these kinds of computer attacks include thrill seekers wanting a challenge, common criminals looking for financial gain, industrial spies trying to gain a competitive advantage, and terrorists seeking to cause destruction to further their cause. Each type of perpetrator has different objectives and access to varying resources, and each is willing to accept different levels of risk to accomplish his or her objective. Each perpetrator makes a decision to act in an unethical manner to achieve his or her own personal objectives. Knowing the profile of each set of likely attackers, as shown in Table 3-5, is the first step toward establishing effective countermeasures.

TABLE 3-5 Classifying perpetrators of computer crime

Type of perpetrator	Typical motives
Hackers	Test limits of system and/or gain publicity
Crackers	Cause problems, steal data, and corrupt systems
Malicious insiders	Gain financially and/or disrupt company's information systems and business operations
Industrial spies	Capture trade secrets and gain competitive advantage
Cybercriminals	Gain financially
Hacktivists	Promote political ideology
Cyberterrorists	Destroy infrastructure components of financial institutions, utilities, and emergency response units

Source Line: Course Technology/Cengage Learning.

Hackers and Crackers

Hackers test the limitations of information systems out of intellectual curiosity—to see whether they can gain access and how far they can go. They have at least a basic understanding of information systems and security features, and much of their motivation comes from a desire to learn even more. The term *hacker* has evolved over the years, leading to its negative connotation today rather than the positive one it used to have. While there is still a vocal minority who believe that hackers perform a service by identifying security weaknesses, most people now believe that a hacker does not have the right to explore public or private networks.

Some hackers are smart and talented, but many are technically inept and are referred to as **lamers** or **script kiddies** by more skilled hackers. Surprisingly, hackers have a wealth of available resources to hone their skills—online chat groups, Web sites, downloadable hacker tools, and even hacker conventions (such as DEFCON, an annual gathering in Las Vegas).

Malicious Insiders

A major security concern for companies is the **malicious insider**—an ever-present and extremely dangerous adversary. Companies are exposed to a wide range of fraud risks, including diversion of company funds, theft of assets, fraud connected with bidding processes, invoice and payment fraud, computer fraud, and credit card fraud. Not surprisingly, fraud that occurs within an organization is usually due to weaknesses in its internal control procedures. As a result, many frauds are discovered by chance and by outsiders—via tips, through resolving payment issues with contractors or suppliers, or during a change of management—rather than through control procedures. Often, frauds involve some form of **collusion**, or cooperation, between an employee and an outsider. For example, an employee in Accounts Payable might engage in collusion with a company supplier. Each time the supplier submits an invoice, the Accounts Payable employee adds $1,000 to the amount approved for payment. The inflated payment is received by the supplier, and the two split the extra money.

Insiders are not necessarily employees; they can also be consultants and contractors. The risk tolerance of insiders depends on whether they are motivated by financial gain, revenge on their employers, or publicity.

Malicious insiders are extremely difficult to detect or stop because they are often authorized to access the very systems they abuse. Although insiders are less likely to attack systems than outside hackers or crackers are, the company's systems are far more vulnerable to them. Most computer security measures are designed to stop external attackers but are nearly powerless against insiders. Insiders have knowledge of individual systems, which often includes the procedures to gain access to login IDs and passwords. Insiders know how the systems work and where the weak points are. Their knowledge of organizational structure and security procedures helps them avoid detection of their actions.

The Saudi Arabian Oil Company (Aramco) is the state-owned oil company of Saudi Arabia. It owns approximately one-fifth of the world's oil reserves and employs more than 55,000 workers in 77 countries.[28] In 2012, the firm was a victim of a cyberattack that erased data on about 30,000 of its personal computers. Security experts believe that the attack was led by a company insider who had privileged access to Aramco's network.[29]

There are several steps organizations can take to reduce the potential for attacks from insiders, including the following:

- Perform a thorough background check as well as psychological and drug testing of candidates for sensitive positions.
- Establish an expectation of regular and ongoing psychological and drug testing as a normal routine for people in sensitive positions.
- Carefully limit the number of people who can perform sensitive operations, and grant only the minimum rights and privileges necessary to perform essential duties.
- Define job roles and procedures so it is not possible for the same person to both initiate and approve an action.
- Periodically rotate employees in sensitive positions so that any unusual procedures can be detected by the replacement.
- Immediately revoke all rights and privileges required to perform old job responsibilities when someone in a sensitive position moves to a new position.
- Implement an ongoing audit process to review key actions and procedures.

Organizations must also be concerned about **negligent insiders**, poorly trained and inadequately managed employees who mean well but have the potential to cause much damage by accident.

Industrial Spies

Industrial spies use illegal means to obtain trade secrets from competitors. In the United States, trade secrets are protected by the Economic Espionage Act of 1996, which makes it a federal crime to use a trade secret for one's own benefit or another's benefit. Trade secrets are most often stolen by insiders, such as disgruntled employees and exemployees.

Competitive intelligence is legally obtained information gathered using sources available to the public. Information is gathered from financial reports, trade journals, public filings, and printed interviews with company officials. **Industrial espionage** involves using illegal means to obtain information that is not available to the public. Participants might place a wiretap on the phones of key company officials, bug a conference room, or break into a research and development facility to steal confidential test results. An unethical firm may spend a few thousand dollars to hire an industrial spy to steal trade secrets that can be worth a thousand times that amount. The industrial spy avoids taking risks that would expose his employer, as the employer's reputation (an intangible but valuable item) would be considerably damaged if the espionage were discovered. Industrial espionage can involve the theft of new product designs, production data, marketing information, or new software source code. For example, a virus called "ACAD/Medre.A" was used to steal thousands of blueprints from companies based mainly in Peru and secretly email them to two Chinese firms. The virus targets AutoCAD software used by engineers and industrial designers to create drawings of new products, equipment, and plant layouts. It is suspected that the virus was initially distributed via an innocent looking AutoCAD template emailed to Peruvian companies. The virus sends a copy of every new design to the virus owners, giving them full "access to the designs even before they go into production."[30]

Cybercriminals

Information technology provides a new and highly profitable venue for **cybercriminals**, who are attracted to the use of information technology for its ease in reaching millions of potential victims. Cybercriminals are motivated by the potential for monetary gain and hack into computers to steal, often by transferring money from one account to another to another—leaving a hopelessly complicated trail for law enforcement officers to follow. Cybercriminals also engage in all forms of computer fraud—stealing and reselling credit card numbers, personal identities, and cell phone IDs. Because the potential for monetary gain is high, they can afford to spend large sums of money to buy the technical expertise and access they need from unethical insiders.

The use of stolen credit card information is a favorite ploy of computer criminals. Fraud rates are highest for merchants who sell downloadable software or expensive items such as electronics and jewelry (because of their high resale value). Credit card companies are so concerned about making consumers feel safe while shopping online that many are marketing new and exclusive zero-liability programs, although the Fair Credit Billing Act limits consumer liability to only $50 of unauthorized charges. When a charge is made fraudulently in a retail store, the bank that issued the credit card must pay the fraudulent charges. For fraudulent credit card transactions over the Internet, the Web merchant absorbs the cost.

A high rate of disputed transactions, known as charge-backs, can greatly reduce a Web merchant's profit margin. However, the permanent loss of revenue caused by lost customer trust has far more impact than the costs of fraudulent purchases and bolstering security. Most companies are afraid to admit publicly that they have been hit by online fraud or hackers because they don't want to hurt their reputations.

In a major case of identity theft, MasterCard recently notified financial institutions that a data breach had occurred at one of its third-party payment processors that could enable the thieves to duplicate the cards of millions of its cardholders. (A **data breach** is the unintended release of sensitive data or the access of sensitive data by unauthorized individuals.) It is likely that data of Visa card holders was also stolen. The total number of card holders that might be affected and the banks notified were not revealed.[31]

To reduce the potential for online credit card fraud, most e-commerce Web sites use some form of encryption technology to protect information as it comes in from the consumer. Some also verify the address submitted online against the one the issuing bank has on file, although the merchant may inadvertently throw out legitimate orders as a result—for example, a consumer might place a legitimate order but request shipment to a different address because it is a gift. Another security technique is to ask for a card verification value (CVV), the three-digit number above the signature panel on the back of a credit card. This technique makes it impossible to make purchases with a credit card number stolen online. An additional security option is transaction-risk scoring software, which keeps track of a customer's historical shopping patterns and notes deviations from the norm. For example, say that you have never been to a casino and your credit card information is being used at Caesar's Palace at 2:00 a.m. The transaction-risk score would go up dramatically, so much so that the transaction might be declined.

Some card issuers are issuing debit and credit cards in the form of **smart cards**, which contain a memory chip that is updated with encrypted data every time the card is used.

This encrypted data might include the user's account identification and the amount of credit remaining. To use a smart card for online transactions, consumers must purchase a card reader that attaches to their personal computers and enter a personal identification number to gain access to the account. Although smart cards are used widely in Europe, they are not as popular in the United States because of the changeover costs for merchants.

Hacktivists and Cyberterrorists

Hacktivism, a combination of the words *hacking* and *activism*, is hacking to achieve a political or social goal. A **cyberterrorist** launches computer-based attacks against other computers or networks in an attempt to intimidate or coerce an organization in order to advance certain political or social objectives. Cyberterrorists are more extreme in their goals than hacktivists, although there is no clear demarcation line. Because of the Internet, cyberattacks can easily originate from foreign countries, making detection and retaliation much more difficult. Cyberterrorists seek to cause harm rather than gather information, and they use techniques that destroy or disrupt services. They are extremely dangerous, consider themselves to be at war, have a very high acceptance of risk, and seek maximum impact.

In late 2012, the hacktivist group Parastoo hacked into the International Atomic Energy Agency (IAEA) network and stole the email addresses of 167 experts working with the agency. The group then posted an online statement demanding that the experts petition the IAEA to investigate what it considered to be "beyond-harmful operations" at Israel's Negev Nuclear Research Center. Parastoo threatened to expose the whereabouts of these experts, as well as other personal information, if they failed to act.[32]

Federal Laws for Prosecuting Computer Attacks

Computers came into use in the 1950s. Initially, there were no laws that pertained strictly to computer-related crimes. For example, if a group of criminals entered a bank and stole money at gunpoint, they could be captured and charged with robbery—the crime of seizing property through violence or intimidation. However, by the mid-1970s, it was possible to access a bank's computer remotely using a terminal (a keyboard and monitor), modem, and telephone line. A knowledgeable person could then transfer money (in the form of computer bits) from accounts in that bank to an account in another bank. This act did not fit the definition of robbery, and the traditional laws were no longer adequate to punish criminals who used computer modems.

Over the years, several laws have been enacted to help prosecute those responsible for computer-related crime; these are summarized in Table 3-6. For example, the USA Patriot Act defines cyberterrorism as hacking attempts that cause $5,000 in aggregate damage in one year to medical equipment, or that cause injury to any person. 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.)

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.

TABLE 3-6 Federal laws that address computer crime

Federal law	Subject area
USA Patriot Act	Defines cyberterrorism and associated penalties
Identity Theft and Assumption Deterrence Act (U.S. Code Title 18, Section 1028)	Makes identity theft a federal crime with penalties up to 15 years imprisonment and a maximum fine of $250,000
Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029)	False claims regarding unauthorized use of credit cards
Computer Fraud and Abuse Act (U.S. Code Title 18, Section 1030)	Fraud and related activities in association with computers: • 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
Stored Wire and Electronic Communications and Transactional Records Access Statutes (U.S. Code Title 18, Chapter 121)	Unlawful access to stored communications to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage

Source Line: Course Technology/Cengage Learning.

IMPLEMENTING TRUSTWORTHY COMPUTING

Trustworthy computing is a method of computing that delivers secure, private, and reliable computing experiences based on sound business practices—which is what organizations worldwide are demanding today. Software and hardware manufacturers, consultants, and programmers all understand that this is a priority for their customers. For example, Microsoft has pledged to deliver on a trustworthy computing initiative designed to improve trust in its software products, as summarized in Figure 3-4 and Table 3-7.[33]

The security of any system or network is a combination of technology, policy, and people and requires a wide range of activities to be effective. As the Committee on Improving Cybersecurity Research in the United States wrote in a report for the National Academy of Sciences, "Society ultimately expects computer systems to be trustworthy—that is, that they do what is required and expected of them despite environmental disruption, human user and operator errors, and attacks by hostile parties, and that they not do other things."[34] A strong security program begins by assessing threats to the organization's computers and network, identifying actions that address the most serious vulnerabilities, and educating end users about the risks involved and the actions they must take to prevent a security incident. An organization's IT security group must lead the effort to prevent security breaches by implementing security policies and procedures, as well as effectively employing available hardware and software tools. However, no security system

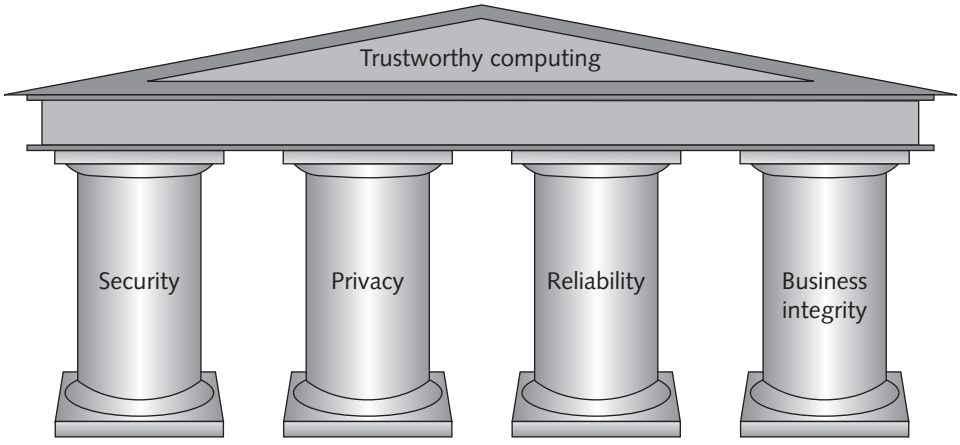


FIGURE 3-4 Microsoft's four pillars of trustworthy computing
Source Line: Course Technology/Cengage Learning.

TABLE 3-7 Actions taken by Microsoft to support trustworthy computing

Pillar	Actions taken by Microsoft
Security	Invest in the expertise and technology required to create a trustworthy environment.
	Work with law enforcement agencies, industry experts, academia, and private sectors to create and enforce secure computing.
	Develop trust by educating consumers on secure computing.
Privacy	Make privacy a priority in the design, development, and testing of products.
	Contribute to standards and policies created by industry organizations and government.
	Provide users with a sense of control over their personal information.
Reliability	Build systems so that (1) they continue to provide service in the face of internal or external disruptions; (2) they can be easily restored to a previously known state with no data loss in the event of a disruption; (3) they provide accurate and timely service whenever needed; (4) required changes and upgrades do not disrupt them; (5) they contain minimal software bugs on release; and (6) they work as expected or promised.
Business integrity	Be responsive—take responsibility for problems and take action to correct them. Be transparent—be open in dealings with customers, keep motives clear, keep promises, and make sure customers know where they stand in dealing with the company.

Source Line: Course Technology/Cengage Learning.

is perfect, so systems and procedures must be monitored to detect a possible intrusion. If an intrusion occurs, there must be a clear reaction plan that addresses notification, evidence protection, activity log maintenance, containment, eradication, and recovery. The following sections discuss these activities.

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 Web site undergoing a distributed denial-of-service attack. Figure 3-5 illustrates a general security risk assessment process developed by ASIS International.

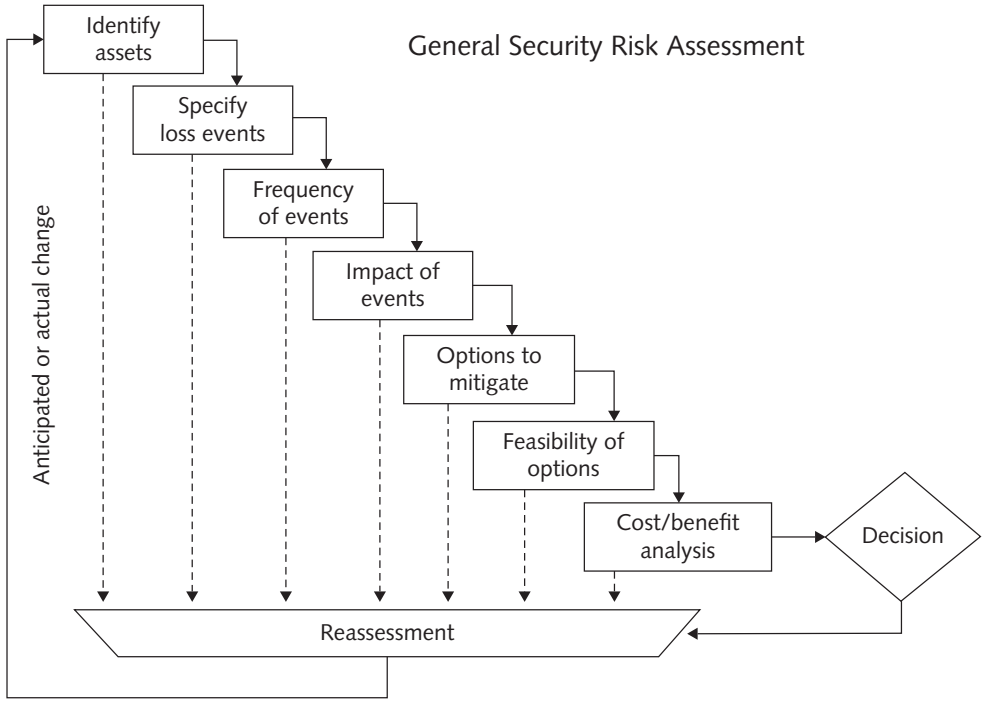


FIGURE 3-5 General security risk assessment

Source Line: General Security Risk Assessment Guidelines, ASIS International (2003). See the Standards and Guidelines page of the ASIS International website (www.asisonline.org) for revisions and/or updates. Reprinted by permission.

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 distributed denial-of-service 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. For example, installing virus protection on all computers makes it much less likely for a computer to contract a virus. Due to time and resource limitations, most organizations choose to focus on those threats that have a high (relative to all other threats) frequency 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** 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 3-8 illustrates a risk assessment for a hypothetical organization.

TABLE 3-8 Risk assessment for hypothetical company

Adverse event	Business objective threatened	Threat (estimated frequency of event)	Vulnerability (likelihood of damage due to event)	Estimated cost of a successful attack	Risk = Threat × Vulnerability × Estimated cost	Relative priority to be fixed
Distributed denial-of-service attack	24/7 operation of a retail Web site	3 per year	25%	$500,000	$375,000	1
Email attachment with harmful worm	Rapid and reliable communications among employees and suppliers	1,000 per year	.05%	$200,000	$100,000	2
Harmful virus	Employees' use of personal productivity software	2,000 per year	.04%	$50,000	$40,000	3
Invoice and payment fraud	Reliable cash flow	1 per year	10%	$200,000	$20,000	4

Source Line: Course Technology/Cengage Learning.

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

Establishing a Security Policy

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 SANS (SysAdmin, Audit, Network, Security) Institute's Web site 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.* The following is a partial list of the templates available from the SANS Institute:

- *Ethics Policy*—This template defines the means to establish a culture of openness, trust, and integrity in business practices.
- *Information Sensitivity Policy*—This sample policy defines the requirements for classifying and securing the organization's information in a manner appropriate to its level of sensitivity.
- *Risk Assessment Policy*—This template defines the requirements and provides the authority for the information security team to identify, assess, and remediate risks to the organization's information infrastructure associated with conducting business.
- *Personal Communication Devices and Voice-mail Policy*—This sample policy describes security requirements for personal communication devices and voice mail.

Whenever possible, automated system rules should mirror an organization's written policies. 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. However, users will often attempt to circumvent security policies or simply ignore them altogether. For example, manufacturers of network routers urge users to change the default password of their router when they first set it up. A hacker discovered numerous routers around the world that are still using the default password and published a list of these routers and their IP addresses so that anyone can get into the associated network and wreak havoc.[35]

When applying system security restrictions, there are some trade-offs between ease of use and increased security; however, when a decision is made to favor ease of use, security incidents sometimes increase. As security techniques continue to advance in sophistication, they become more transparent to end users.

The use of email attachments is a critical security issue that should be addressed in every organization's security policy. Sophisticated attackers may be able to penetrate a network via email attachments, regardless of the existence of a firewall and other security measures. As a result, some companies have chosen to block any incoming mail that has a file attachment, which greatly reduces their vulnerability. Some companies allow employees to receive and open email with attachments, but only if the email is expected

and from someone known by the recipient. Such a policy can be risky, however, because worms often use the address book of their victims to generate emails to a target audience.

Another growing area of concern 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 to gain access to their corporate network.

A **virtual private network (VPN)** works by using the Internet to relay communications; it maintains privacy through security procedures and tunneling protocols, which encrypt data at the sending end and decrypt it at the receiving end. An additional level of security involves encrypting the originating and receiving network addresses. Because of the ease of loss or theft, many organizations encrypt all sensitive corporate data stored on handhelds and laptops. Unfortunately, it is hard to apply a single, simple approach to securing all handheld devices because so many manufacturers and models exist.

Educating Employees and Contract Workers

An ongoing security problem for companies is creating and enhancing user awareness of security policies. Employees and contract workers must be educated about the importance of security so that they will be motivated to understand and follow the 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)

Prevention

No organization can ever be completely secure from attack. The key is to implement a layered security solution to make computer break-ins so difficult that an attacker eventually gives up. In a layered solution, if an attacker breaks through one layer of security, there is another layer to overcome. These layers of protective measures are explained in more detail in the following sections.

Installing a Corporate Firewall

Installation of a corporate firewall is the most common security precaution taken by businesses. A firewall stands guard between an organization's internal network and the Internet, and it limits network access based on the organization's access policy.

Firewalls can be established through the use of software, hardware, or a combination of both. Any Internet traffic that is not explicitly permitted into the internal network is denied entry. Similarly, most firewalls can be configured so that internal network users can be blocked from gaining access to certain Web sites based on such content as sex and violence. Most firewalls can also be configured to block instant messaging, access to newsgroups, and other Internet activities.

Installing a firewall can lead to another serious security issue—complacency. For example, a firewall cannot prevent a worm from entering the network as an email attachment. Most firewalls are configured to allow email and benign-looking attachments to reach their intended recipient.

Table 3-9 lists some of the top-rated firewall software used to protect personal computers. The software suites below include antivirus, firewall, antispam, parental control, and phishing protection capabilities and sell for $70 to $90 per single user license.

TABLE 3-9 Top-rated firewall software for personal computers

Software	Vendor
Norton 360 v 6.0	Symantec
Norton Internet Security (2013)	Symantec
Kaspersky PURE 2.0 Total Security	Kaspersky
Kaspersky Internet Security 2013	Kaspersky
Zone Alarm Extreme Security 2012	Check Point
Zone Alarm Free	Check Point

Source Line: Neil J. Rubenking, "The Best Security Suites of 2013," *PC Magazine*, September 19, 2012, www.pcmag.com/article2/0,2817,2369749,00.asp.

Intrusion Detection Systems

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 3-6). Such activities usually signal an attempt to breach the integrity of the system or to limit the availability of network resources.

Knowledge-based approaches and behavior-based approaches are two fundamentally different approaches to intrusion detection. Knowledge-based intrusion detection systems 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 intrusion detection system models normal behavior of a system and its users from reference information collected by various means. The intrusion detection system compares current activity with 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 she has never before used.

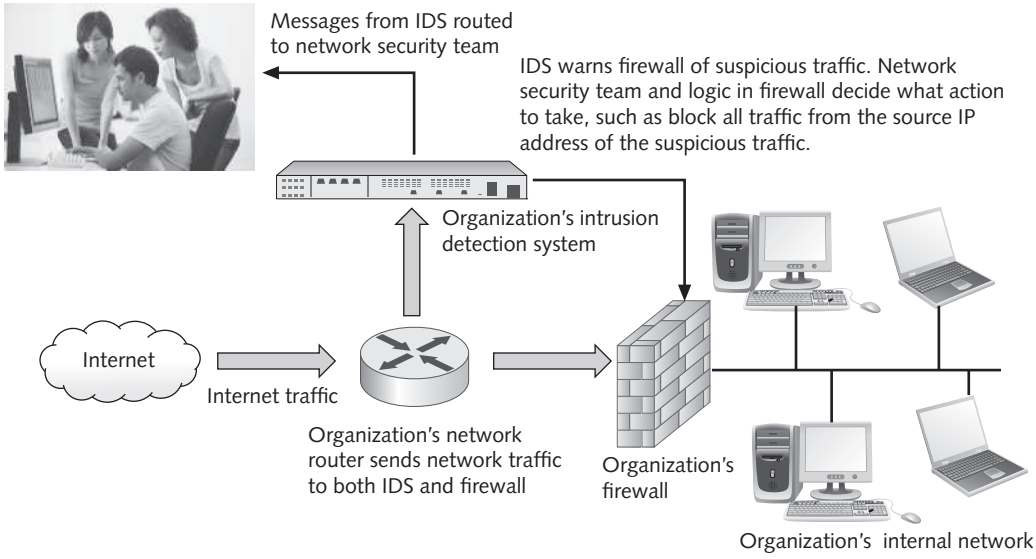


FIGURE 3-6 Intrusion detection system
Credit: © Monkey Business Images/Shutterstock.com.

Installing Antivirus Software on Personal Computers

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 viruslike 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.

The **United States Computer Emergency Readiness Team (US-CERT)** is a partnership between the Department of Homeland Security and the public and private sectors—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 (over 500 new viruses and worms are developed each month[36]). According to US-CERT, most of the virus and worm attacks that the team analyzes 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 Web sites 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. In fact, in recent testing of 13 antivirus software packages, only two such programs (Kaspersky Internet Security 2012 and Alwil Avast Internet

Security 2012) blocked more than 80 percent of a sample of known exploits, according to the independent testing firm NSS Labs.[37]

Implementing Safeguards Against Attacks by Malicious Insiders

User accounts that remain active after employees leave a company are another potential security risk. To reduce the threat of attack by malicious insiders, IT staff must promptly delete the computer accounts, login IDs, and passwords of departing employees and contractors.

Organizations also need to define employee roles carefully and separate key responsibilities properly, so that a single person is not responsible for accomplishing a task that has high security implications. For example, it would not make sense to allow an employee to initiate as well as approve purchase orders. That would allow an employee to input large invoices on behalf of a "friendly vendor," approve the invoices for payment, and then disappear from the company to split the money with the vendor. In addition to separating duties, many organizations frequently rotate people in sensitive positions to prevent potential insider crimes.

Another important safeguard is to create roles and user accounts so that users 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 Human Resources 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 Finance 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.

Defending Against Cyberterrorism

In the face of increasing risks of cyberterrorism, organizations need to be aware of the resources available to help them combat this serious threat. The **Department of Homeland Security (DHS)** leads the federal government's efforts in "securing civilian government computer systems, and works with industry and state, local, tribal, and territorial governments to secure critical infrastructure and information systems."[38] According to the department's Web site, the DHS works to "analyze and reduce cyberthreats and vulnerabilities; distribute threat warnings; and coordinate the response to cyberincidents to ensure that our computers, networks, and cybersystems remain safe."[39]

The Protected Critical Infrastructure Information Program encourages private industry to share confidential information about the nation's critical infrastructure with the DHS under the assurance that the information will be protected from public disclosure. This allows private industry and DHS to work jointly to identify threats and vulnerabilities and to develop countermeasures and defensive strategies.[40]

Critical infrastructures include telecommunications, energy, banking and finance, water, government operations, and emergency services. Specific targets might include telephone-switching systems, an electric power grid that serves major portions of a geographic region, or an air traffic control center that ensures airplanes can take off and land

safely. Successful cyberattacks on such targets could cause widespread and massive disruptions to society. Some computer security experts believe that cyberterrorism attacks could be used to create further problems following a major act of terrorism by reducing the ability of fire and emergency teams to respond.

Addressing the Most Critical Internet Security Threats

The overwhelming majority of successful computer attacks takes advantage of well-known vulnerabilities. Computer attackers know that many organizations are slow to fix problems, which makes scanning the Internet for vulnerable systems an effective attack strategy. The rampant and destructive spread of worms, such as Blaster, Slammer, and Code Red, was made possible by the exploitation of known but unpatched vulnerabilities. US-CERT regularly updates a summary of the most frequent, high-impact vulnerabilities being reported to them. You can read this summary at *www.us-cert.gov/current.* The actions required to address these issues include installing a known patch to the software and keeping applications and operating systems up to date. Those responsible for computer security must make it a priority to prevent attacks using these vulnerabilities.

Conducting Periodic IT 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 need 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.

The Information Protection Assessment kit is an assessment tool available from the Computer Security Institute, an organization for information security professionals. The kit can be accessed at *http://gocsi.com/ipak* and is formatted as a Microsoft Excel® spreadsheet that covers 15 categories of security issues (e.g., physical security, business process controls, network security controls). Each category has approximately 20 statements used to rate the effectiveness of security for that category. Organizations can complete the survey to get a clear measure of the effectiveness of their security programs and to define areas that need improvement.

Detection

Even when preventive measures are implemented, no organization is completely secure from a determined attack. Thus, organizations should implement detection systems to catch intruders in the act. Organizations often employ an intrusion detection system to minimize the impact of intruders.

Response

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.

DreamHost (*http://dreamhost.com*) is a Web site hosting service that hosts more than 1 million domains on 1,500 servers.[41] Early in 2012, its IDS system detected that its servers were being attacked by an exploit not previously known nor prevented by its other security systems. The IDS alerted the DreamHost security team who quickly identified the means of illegal access and shut it down. The security team determined that some customer passwords may have been compromised, so the team immediately initiated a forced reset of all customer passwords to prevent any malicious activity on any customer Web site. They also sent out customer notifications informing them of the situation.[42] A quick response allows companies to more quickly get control of a security incident, while also limiting the potential damage to customers.

Incident Notification

A key element of any response plan is to define who to notify and who not to notify. 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 need to be kept informed and up to date without using systems connected to the compromised system. The intruder may be monitoring these systems and email 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 to be unethical and harmful, a number of state and federal laws have been passed to force organizations to reveal when customer data has been breached. These laws will be discussed further in the next chapter.

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 data 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 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 virus. 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, the group must create a new backup. Throughout this process, a log should be kept of all actions taken. This will prove helpful during the 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. This process should 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 include the following:

- IP address and name of host computer(s) involved
- The date and time when the incident was discovered
- The length of the incident
- 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, etc.)
- Whether the data is 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 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 Web site 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. Discussing 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 decide if 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.

Symantec, a leading provider of security software, was attacked in 2006 and the source code for several of its products was stolen. The firm did not report the embarrassing incident until six years later. The delay in reporting the breach raised customer concern and put the company on the defensive.[43]

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 has 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.

Proper handling of a computer forensics investigation is the key to fighting computer crime successfully in a court of law. In addition, extensive training and certification increases the stature of a computer forensics investigator in a court of law. There are numerous certifications related 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 forensics 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.

A computer forensics investigator must be knowledgeable about the various laws that apply to the gathering of criminal evidence; see Table 3-10 for a partial list.

TABLE 3-10 Partial list of constitutional amendments and statutes governing the collection of evidence

Law	Subject area
Fourth Amendment	Protects against unreasonable search and seizure
Fifth Amendment	Provides protection from self-incrimination
Wiretap Act (18 U.S.C. 2510-2522)	Regulates the collection of the content of wire and electronic communications
Pen Registers and Trap and Trace Devices Statute (18 U.S.C. 3121-27)	Provides restrictions on the use of pen registers and trap and trace devices (a pen register is a device that records all numbers dialed from a particular phone; a trap and trace device shows the phone numbers that have made calls to a specific phone)
Stored Wire and Electronic Communications Act (18 U.S.C 2701-120)	Addresses the disclosure of stored wired and electronic communications and transaction records by Internet service providers

Source Line: Course Technology/Cengage Learning.

Violation of any one of these laws could result in a case being thrown out of court. It could even result in the investigator being charged with a federal felony, punishable by a fine and/or imprisonment.

Table 3-11 provides a manager's checklist for evaluating an organization's readiness for a security incident. The preferred answer to each question is *yes*.

TABLE 3-11 Manager's checklist for evaluating an organization's readiness for a security incident

Question	Yes	No
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: • Email with executable file attachments? • Wireless networks and devices? • Use of smartphones deployed as part of corporate rollouts as well as those bought by end users?		
Is there an effective security education program for employees and contract workers?		
Has a layered security solution been implemented to prevent break-ins?		
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 and contractors promptly deleted?		
Is there a well-defined separation of employee responsibilities?		
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?		

Source Line: Course Technology/Cengage Learning.

Summary

- The security of information technology used in business is of the utmost importance, but it must be balanced against other business needs and issues.
- Increasing complexity, higher computer user expectations, expanding and changing systems, and increased reliance on software with known vulnerabilities have caused a dramatic increase in the number, variety, and impact of security incidents.
- Viruses, worms, Trojan horses, spam, distributed denial-of-service attacks, rootkits, phishing, spear-phishing, smishing, and vishing are among the most common computer exploits.
- A successful computer exploit aimed at several organizations can have a cost impact of more than $1 billion.
- There are many different kinds of people who launch computer attacks, including the hacker, cracker, malicious insider, industrial spy, cybercriminal, hacktivist, and cyberterrorist. Each type has a different motivation.
- Over the years, several laws have been enacted to prosecute those responsible for computer-related crime, including the USA Patriot Act, the Computer Fraud and Abuse Act, the Identity Theft and Assumption Deterrence Act, the Fraud and Related Activity in Connection with Access Devices Statute, and the Stored Wire and Electronic Communications and Transactional Record Access Statutes.
- Trustworthy computing is a method of computing that delivers secure, private, and reliable computing experiences based on sound business practices.
- The security of any system is a combination of technology, policy, and people, and it requires a wide range of activities to be effective.
- A strong security program begins by assessing threats to the organization's computers and network, identifying actions that address the most serious vulnerabilities, and educating users about the risks involved and the actions they must take to prevent a security incident.
- The IT security group must lead the effort to implement security policies and procedures, along with hardware and software tools to help prevent security breaches.
- No organization can ever be completely secure from 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.
- No security system is perfect, so systems and procedures must be monitored to detect a possible intrusion.
- If an intrusion occurs, there must be a clear reaction plan that addresses notification, evidence protection, activity log maintenance, containment, eradication, and recovery.
- Special measures must be taken to implement safeguards against attacks by malicious insiders and to defend against cyberterrorism.
- Organizations must implement fixes against well-known vulnerabilities.
- Organizations should conduct periodic IT security audits.
- Organizations need to be knowledgeable of and have access to trained experts in computer forensics.

Key Terms

antivirus software
botnet
bring your own device (BYOD)
CAPTCHA
cloud computing
collusion
competitive intelligence
computer forensics
Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act
cybercriminal
cyberterrorist
data breach
Department of Homeland Security
distributed denial-of-service (DDoS) attack
exploit
hacker
hacktivism
industrial espionage
industrial spy
intrusion detection system (IDS)
lamer
logic bomb
malicious insider
negligent insider
phishing
ransomware
reasonable assurance
risk assessment
rootkit
script kiddie
security audit
security policy
smart card
smishing
spam
spear-phishing
Trojan horse
trustworthy computing
United States Computer Emergency Readiness Team (US-CERT)
virtual machine
virtual private network (VPN)
virtualization software
virus
virus signature
vishing
worm
zero-day attack
zombie

Self-Assessment Questions

The answers to the Self-Assessment Questions can be found in Appendix B.

1. According to the 2010/11 CSI Computer Crime and Security Survey, which of the following was the most common security incident?
   a. being fraudulently misrepresented as a sender of email messages requesting personal information
   b. malware infection
   c. laptop or mobile hardware theft
   d. employees, abuse of Internet access or email

2. Computer security incidents occur around the world, with personal computer users in developing countries being exposed to the greatest risk of their computers being infected by malware. True or False?
3. An attack on an information system that takes advantage of a vulnerability is called a(n) _____.
4. _____ software operates in a software layer that runs on top of the operating system and enables multiple virtual machines each with their own operating system to run on a single computer.
5. The number of new software vulnerabilities identified has steadily increased each year since 2006. True or False?
6. A(n) _____ takes places before the security community or software developer knows about the vulnerability or has been able to repair it.
7. Software that generates and grades tests that humans can pass but that all but the most sophisticated computer programs cannot is called _____.
8. _____ is a form of malware that, if a user unknowingly downloads it to his or her smartphone, takes control of the device and its data until the owner agrees to pay a ransom to the attacker.
9. A(n) _____ 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.
10. A(n) _____ is malicious code hidden inside a seemingly harmless program.
11. A(n) _____ is a large group of computers controlled from one or more remote locations by hackers, without the knowledge or consent of their owners.
12. _____ is a method of computing that delivers secure, private, and reliable computing experiences.
13. The process of assessing security-related risks from both internal and external threats to an organization's computers and networks is called a(n) _____.
14. The written statement that defines an organization's security requirements as well as the controls and sanctions used to meet those requirements is known as a:
    a. risk assessment
    b. security policy
    c. firewall
    d. none of the above
15. Implementation of a strong firewall provides adequate security for almost any network. True or False?
16. In a security incident, the primary goal must be to monitor and catch the intruder. True or False?

Discussion Questions

1. Develop a strong argument against the adoption of a bring your own device (BYOD) policy for a large financial services organization. Now develop a strong argument in favor of the adoption of such a policy.
2. A successful distributed denial-of-service 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 fined or otherwise punished as a means of encouraging people to better safeguard their computers? Why or why not?
3. Provide a real example or describe a hypothetical situation where a legitimate organization used spam in an effective and nonintrusive manner to promote a product or service.
4. Some IT security personnel believe that their organizations should employ former computer criminals to identify weaknesses in their organizations' security defenses. Do you agree? Why or why not?
5. You have been assigned to be a computer security trainer for your firm's 2,000 employees and contract workers. What are the key topics you would cover in your initial one-hour basic training program for non-IT personnel? What sort of additional security-related training might be appropriate once people have the basics covered?
6. Your computer science instructor has assigned a semester-long project to develop a zero-day exploit for the Windows 8 operating system. Do you think this is an appropriate class project? Why or why not?
7. How should a nonprofit charity handle the loss of personal data about its donors? Should law enforcement be involved? Should donors be informed?
8. Draft a legitimate-looking phishing email that would strongly tempt its recipients to click on a link to a Web site or open an email attachment.
9. What is the difference between industrial spying and the gathering of competitive intelligence? Is the use of competitive intelligence ethical or unethical? Why?
10. 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?
11. Outline action steps necessary to implement trustworthy computing.
12. What is the difference between risk assessment and an IT security audit?

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 one of the top students in your university's computer science program of 200 students. You are surprised when you are met after class by two representatives from a federal intelligence agency. Over dinner, they talk to you about the increasing threat of cyberterrorist attacks launched on the United States by foreign countries and the need to counter those attacks. They offer you a position on the agency's supersecret

cyberterrorism unit, at a starting salary 50 percent higher than you know other computer science graduates are being offered. Your role would be to both develop and defend against new zero-day exploits that could be used to plant malware in the software used by the government and military computers. Would such a role be of interest to you? What questions might you ask to determine if you would accept their offer of employment?

2. You are the CFO of a sporting goods manufacturer and distributor. Your firm has annual sales exceeding $500 million, with roughly 25 percent of your sales coming from online purchases. Today, your firm's Web site was not operational for almost an hour. The IT group informed you that the site was the target of a distributed denial-of-service attack. You are shocked by an anonymous call later in the day in which a man tells you that your site will continue to be attacked unmercifully unless you pay him $250,000 to stop the attacks. What do you say to the blackmailer?
3. You are a member of the Human Resources Department of a three-year-old software manufacturer that has several products and annual revenue in excess of $500 million. You've just received a request from the manager of software development to hire three notorious crackers to probe your company's software products in an attempt to identify any vulnerabilities. The reasoning is that if anyone could find a vulnerability in your software, they could. This will give your firm a head start on developing patches to fix the problems before anyone can exploit them. You're not sure, and you feel uneasy about hiring people with criminal records and connections to unsavory members of the hacker/cracker community. What would you do?
4. Imagine that you have decided on a career in computer forensics. Do research to determine typical starting positions and salaries for someone with a four-year degree in computer forensics. Do further research to find three universities that offer four-year degrees specializing in computer forensics. Compare the three programs, and choose the best one. Why did you choose this university?
5. You are the CFO of a midsized manufacturing firm. You have heard nothing but positive comments about the new CIO you hired three months ago. As you watch 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 computer security improvements will be $300,000. 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 this project. In addition, the $300,000 is above your spending authorization and will require approval by the CEO. This will force you to defend the expenditure, and you are not sure how to do this. You wonder if this much spending on security is really required. How can you sort out what really needs to be done without appearing to be micro-managing or discouraging the new CIO? How do you proceed?
6. Do research to capture several opinions on the effectiveness of the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act. Would you recommend any changes to this act? If so, what changes would you like to see implemented and why?
7. It appears that someone is using your firm's corporate directory—which includes job titles and email addresses—to contact senior managers and directors via email. The email

requests that the recipient click on a URL, which leads to a Web site that looks as if it were designed by your Human Resources organization. Once at this phony Web site, the employees are asked to confirm the bank and account number to be used for electronic deposit of their annual bonus check. You are a member of IT security for the firm. What can you do?

8. You are a member of the application development organization for a small but rapidly growing software company that produces patient billing applications for doctors' offices. During work on the next release of your firm's first and only software product, you discover a small programming glitch in the current release that could pose a security risk to users. The probability of the problem being discovered is low, but, if it is exposed, the potential impact on your firm's 100 or so customers could be substantial: Hackers could access private patient data and change billing records. The problem will be corrected in the next release, scheduled to come out in three months, but you are concerned about what should be done for the users of the current release.

   The problem has come at the worst possible time. The firm is currently seeking approval for a $10 million loan to raise enough cash to continue operations until revenue from the sales of its just-released product offsets expenses. In addition, the effort to develop and distribute the patch, to communicate with users, and to deal with any fallout will place a major drain on your small development staff, delaying the next software release by at least two months. You have your regularly scheduled quarterly meeting with the manager of application development this afternoon; what will you say about this problem?

Cases

1. Defending Against Distributed Denial-of-Service Attacks

A DDoS attack can easily cost an organization tens of thousands of dollars per minute in lost revenue and worker productivity. In addition, in the fallout from such an attack, an organization may find its customers switching to competitors due to a loss of confidence resulting from the bad publicity. Financial and travel service firms and various e-commerce Web sites are frequent targets of DDoS attacks.

During the fall of 2012, powerful DDoS attacks were directed at the Web servers of several major U.S. banks. The DDoS attack directed 65 Gbps of data traffic at each bank server—the network equivalent of an F5 hurricane—effectively making the server inaccessible to customers. The attack repeated itself at one bank after another. Over the course of a few weeks, Bank of America, Capital One, JPMorgan Chase, PNC Financial Services, Regions Financial, Sun Trust, US Bank, and Wells Fargo were all hit. Particularly alarming is that the banks were not able to completely fend off the attacks—the attackers simply stopped on their own to avoid being identified. The parties responsible for these attacks have not been positively identified, but suspects include Hamas, an Islamic group called the Izz ad-Din Al-Qassam Cyber Fighters, the hacktivist group Anonymous, cybercriminals based in Eastern Europe, and hackers in Saudi Arabia and Iran.[44]

SpaFinder is a spa and wellness company that sells spa, wellness, and beauty gift cards and rewards programs that draw millions of clients to its global network of spas, fitness studios, and wellness practitioners.[45] A recent DDoS attack hit SpaFinder's 24/7 call center, making it

impossible for customers to access the Web site to view content, make purchases, redeem gift certificates, or spend rewards points. SpaFinder's Web hosting service was unable to deal with the attack. In desperation, SpaFinder technical support people contacted a DDoS mitigation service company that was able to get their site back up and running in less than 24 hours.[46]

DDoS mitigation service organizations monitor clients' network equipment for signs of a DDoS attack. If such an attack is detected, all traffic is rerouted from the client Web site to the service provider over a dedicated high-speed network link for traffic "scrubbing." This process allows the service provider to use powerful servers to inspect the data traffic for anomalies. All legitimate traffic is forwarded back to the customer for routine processing; all attack traffic is dropped.

In addition to contracting with a DDoS mitigation service provider, security experts recommend that organizations (1) develop and practice a standard operating procedure to follow in the event of a DDoS attack; (2) maintain contact information for their ISP and hosting providers that includes names and phone numbers for whoever should be contacted during a DDoS attack and what information they will need; and (3) prioritize network services to identify what services could be turned off or blocked if needed to limit the effects of the attack.[47]

Discussion Questions

1. Outline a quantitative approach for justifying the use of a DDoS mitigation service to protect an e-commerce company such as SpaFinder. Can you identify any nonfinancial reasons to subscribe to a DDoS mitigation service? If so, what are they?
2. Identify three potential kinds of DDoS attackers of an e-commerce company such as SpaFinder. What would be the motive for each of these attackers?
3. Do research on the Web to find three DDoS mitigation service providers. How are their services similar? How are they different? Which DDoS service provider do you think is the best?

2. Anonymous and Social Hacktivism

The popular conception of hackers is one of young men sitting in dark basement rooms for hours upon end, surrounded by empty takeout containers: alone and unaffiliated. Individual hackers rarely influence history, the actions of large corporations, or the governments of the world—unless they can somehow work together and form a collective. The hacktivist group Anonymous seems to have achieved this goal.[48]

The group's beginnings can be traced back to 2003, when individual hackers began posting proposals for collective action on an Internet forum called 4-chan, a simple image-based bulletin board where anyone can post comments and share images—and one of the least regulated parts of the Internet in the early 2000s. At first, the idea was the adoption of a decentralized online community that could act anonymously, but in a coordinated manner. Group actions were usually aligned toward some nebulous goal, with the primary focus being on the members' own entertainment. For example, Anonymous members hacked the copy-protect codes of DVDs and video games and posted them online. This action enabled other hackers to disable the copy protection and copy these products for free. As the movement grew, some members began to see the potential for greater social and political activity, and social "hacktivism" was born.[49]

Anonymous has no leader or formal decision-making mechanism. “Anyone who wants to can be Anonymous and work toward a set of goals…” a member of Anonymous explained. “We have this agenda that we all agree on and we all coordinate and act, but all act independently toward it, without any want for recognition. We just want to get something that we feel is important done…”[50]

Anonymous’ first move toward a political action came in the form of a distributed denial-of-service (DDoS) attack on the Church of Scientology in 2008. The church had made an attempt to remove an interview with Tom Cruise, a famous church member, from the Internet.[51] The church felt the video injured its image. It succeeded in removing the video from YouTube and other Web sites, but Anonymous posted the video on the Gawker Web site.[52] The effort gave Anonymous a sense of the power it could harness.[53]

As the movement grew, Anonymous expanded its targets and attracted media attention. After the Web site WikiLeaks, which relied on donations to support its operations, released large collections of classified American military documents and diplomatic cables, PayPal, MasterCard, and Bank of America announced that they would no longer process donations to WikiLeaks. This action threatened to put the WikiLeaks Web site out of business. In response, Anonymous launched major DDoS attacks on the Web sites of these financial companies.

In 2012, Anonymous published the names and credit card information of the subscribers to a newsletter published by the international security think tank, Stratfor, which Anonymous viewed as a reactionary force both online and in the real world. Stratfor customer credit cards were used to make over $500,000 in fraudulent donations to various charities.[54] Also in 2012, Anonymous attacked the regime of Syrian president Bashar al-Assad. In this instance, Anonymous went beyond DDoS attacks on government sites and actually set up satellite transmission stations in all the major cities across Syria to serve as independent media centers in anticipation of the Syrian government’s efforts to cut off its citizens from the Internet.[55]

In response to the suicide of Internet activist Aaron Swartz in early 2013, Anonymous briefly corrupted the Web site of the U.S. Sentencing Commission and threatened to release sensitive information concerning the U.S. Department of Justice. Anonymous blamed the justice system for Swartz’s suicide, claiming that prosecutors were pursuing “highly disproportionate sentencing” in cases against some of its members and others, like Swartz, who championed open access to online documents. Swartz was facing federal charges that he stole millions of online documents and could have served up to 35 years in prison.[56]

The group’s strategy of using DDoS attacks and publishing personal information is illegal and has exposed numerous members of the collective to police inquiry and legal problems. The Interpol international policing body has been particularly active in its pursuit of Anonymous members. In early 2012, as part of Interpol’s efforts, 25 Anonymous members were arrested in four different countries.[57] Furthermore, an influential member of the collective, known online as “Sabu,” was recently outed as an FBI informant. After participating in the Stratfor hack, Sabu gave information to the FBI leading to the arrest of several Anonymous senior members.[58] However, after the revelation that one of their own had cooperated with the FBI’s efforts against the group, one member posted the following: “Don’t you get it by now? #Anonymous is an idea. #Anonymous is a movement. It will keep growing, adapting and evolving, no matter what.”[59]

Discussion Questions

1. If you had an opportunity to join Anonymous, would you? Why, or why not?
2. Would you say that Anonymous' actions in support of WikiLeaks were legal? Were these actions ethical? What about their actions to set up satellite transmission stations across Syria?
3. How serious of a threat does Anonymous pose to organizational and government Web sites?

3. Computer Forensics

On September 8, 2009, 25-year-old airport limousine driver and former coffee cart vendor Najibullah Zazi rented a car and drove from Denver to New York City.[60] His car was laden with explosives and bomb-building materials. According to the Department of Justice, Zazi's target was the New York City subway system. It is believed Zazi was planning to work with other operatives over the weekend and detonate the bomb the following week. However, after learning he was under investigation, Zazi dumped the evidence and fled back to Denver. On September 19, the FBI arrested him on charges of willfully making false statements to the FBI. Computer forensics investigators with the FBI found bomb-making instructions and Internet searches for hydrochloric acid on Zazi's laptop computer. Investigators also processed video surveillance of Zazi buying large quantities of bomb-making materials at a beauty supply store.[61] Zazi had also emailed himself detailed notes on constructing explosives during an Al Qaeda training session on constructing explosives that he had attended in Afghanistan in 2008. In February 2010, Zazi pled guilty to conspiracy to use weapons of mass destruction against persons or property in the United States, conspiracy to commit murder in a foreign country, and providing material support to Al Qaeda.[62]

In November 2007, a 900-foot-long container ship traveling through dense fog struck the Bay Bridge in San Francisco Bay. Approximately 58,000 gallons of fuel oil seeped through the 100-foot gash in the hull into the water.[63] Over 2,500 birds died during the spill, and wildlife experts estimated that a total of 20,000 perished as a result of the long-term chemical effects of oil exposure.[64] Prosecutors alleged that the captain had failed to use radar and positional fixes or other official navigation aids.[65] However, the crime extended beyond the captain's negligence. Computer forensics investigators found that computer navigational charts had been doctored after the crash, and falsified records, such as passage planning checklists, had been created on ship computers after the crash.[66] The captain was eventually sentenced to 10 months in federal prison after pleading guilty to violating the Clean Water Act and the Migratory Bird Treaty Act.[67] In 2009, the ship's management company, Fleet Management Company Ltd., agreed to pay $10 million in compensation for violating the Oil Pollution Act of 1990.[68] These two high-profile cases illustrate the central role computer forensics investigators are playing in criminal investigations today. These investigators are at work in both criminal and civil cases exploring everything from murder, kidnapping, and robbery to money laundering and fraud to public corruption, intellectual property theft, and destruction of property by disgruntled employees. Even parties to divorce cases are now making use of computer forensics experts to uncover evidence of infidelity or locate joint funds that have been hidden by one of the spouses.[69]

Yet perhaps the greatest promise of this fast-developing field of investigation is its potential for preventing crime. On November 18, 2010, police arrested a Florida college student, Daniel

Alexander Shana, who had posted on Facebook his plans for carrying out a Columbine High School–type massacre to target people who he felt had bullied him. He boasted that he had purchased a semiautomatic pistol and had registered for a firearms license. Students viewing his Facebook posts reported them to authorities.[70] Computer forensics investigators found that he had viewed videos on Columbine and looked into how to purchase weapons and carry out murder.[71]

As the role of computer forensics has expanded in criminal and civil investigations, the number of jobs available in the fields has grown. The Bureau of Labor Statistics predicts that employment in the field of private detectives and investigators in general will grow by 22 percent between 2008 and 2018.[72] To meet this demand, a number of universities have begun offering undergraduate and graduate degrees in computer forensics. Computer forensics investigators not only analyze, recover, and present data for use as evidence, but also recover emails, passwords, and encrypted or erased data. They must detect intrusions and probe them. Hence, computer forensics investigators require specialized hardware and software, and they must master specific methods and techniques. That said, the Bureau of Labor Statistics advises that a degree in computer science or accounting is more helpful than a degree in criminal justice.[73]

Most computer forensics professionals, enter the field by getting a job with a law enforcement agency and receiving training while on the job.[74] In addition, universities also offer certificates in computer forensics for those already working in the field, and professional organizations host seminars where people interested in the field can gain expertise. Professionals already working in the field can complete a certificate through an online program.

Once computer forensics professionals gain sufficient on-the-job experience, they frequently branch out into the private sector. Licensing requirements vary from state to state, and certification requirements vary from one professional organization to another. The Bureau of Labor Statistics reported that the median salary for private detectives and investigators in 2010 was $42,870. Although the bureau did not track salary information specifically for a computer forensics investigator, professionals in specialized fields are often able to demand higher compensation.[75]

Most important, the Bureau of Labor Statistics reported that job competition in this area is keen. With high-profile cases such as the New York subway bomber and television shows romanticizing the role of computer forensics investigators, it's no wonder people are flocking to the field. Yet even if computer forensics isn't as powerful or glamorous as it appears on TV, the field is becoming more critical to criminal investigation, and increasing expertise will be required as cybercriminals develop more sophisticated means of attack.

Discussion Questions

1. What role did computer forensics play in the high-profile cases of the New York subway bomber and the San Francisco Bay oil spill?
2. Why might computer forensics be more effective at preventing crimes than other forms of criminal investigation?
3. In addition to computer-related training, what other education and background would be ideal for someone who wants to make a career in computer forensics?

End Notes

[1] Dan Goodin, "Mushrooming Ransomware Now Extorts $5 Million a Year," *Ars Technica*, November 8, 2012, http://arstechnica.com/security/2012/11/mushrooming-growth-of-ransomware-extorts-5-million-a-year.

[2] Federal Bureau of Investigation, "New Internet Scam," August 9, 2012, www.fbi.gov/news/stories/2012/august/new-internet-scam.

[3] Dan Goodin, "Mushrooming Ransomware Now Extorts $5 Million a Year," *Ars Technica*, November 8, 2012, http://arstechnica.com/security/2012/11/mushrooming-growth-of-ransomware-extorts-5-million-a-year.

[4] Gavin O'Gorman and Geoff McDonald, "Ransomware: A Growing Menace," Symantec, www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf.

[5] "Inside a 'Reveton' Ransomware Operation," KrebsOnSecurity, August 12, 2012, http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation.

[6] Matthew J. Schwartz, "Ransomware Pays: FBI Updates Reveton Malware Warning," *InformationWeek*, December 3, 2012, www.informationweek.com/security/vulnerabilities/ransomware-pays-fbi-updates-reveton-malw/240143047.

[7] "Trio Arrested in Staffordshire over 'Ransomware' Scam," BBC News Technology, December 14, 2012, www.bbc.co.uk/news/technology-20724810.

[8] Andrew Brandt, "Ransomware Debuts New Java Exploit, Sends Victims Running for MoneyPak Cards," Solera Networks Labs, July 10, 2012, www.soleranetworks.com/blogs/ransomware-debuts-new-java-exploit-sends-victims-running-for-moneypak-cards.

[9] Gavin O'Gorman and Geoff McDonald, "Ransomware: A Growing Menace," Symantec, www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf.

[10] Ricardo Geromel, "Hackers Stole $1 Billion in Brazil, The Worst Prepared Nation to Adopt Cloud Technology," *Forbes*, March 2, 2012, www.forbes.com/fdc/welcome_mjx.shtml.

[11] Barb Goldworm, "Server Virtualizations Expert's Guide," Ziff Davis, March 2012.

[12] Steven Musil, "Oracle Releases Software Update to Fix Java Vulnerability," *CNET*, January 13, 2013, http://news.cnet.com/8301-1009_3-57563730-83/oracle-releases-software-update-to-fix-java-vulnerability/.

[13] Dan Goodin, "Zero-Day Attacks Are Meaner, More Rampant Than We Ever Thought," *ARS Technica*, October 16, 2012, http://arstechnica.com/security/2012/10/zero-day-attacks-are-meaner-and-more-plentiful-than-thought.

[14] David Goldman, "Malware Attacks on the Rise," *CNN Money*, September 4, 2012, http://money.cnn.com/2012/09/04/technology/malware-cyber-attacks/index.html.

[15] Ken Presti, "Kaspersky: SMS Trojans Account for Over Half of Smartphone Malware," *CRN*, November 2, 2012, www.crn.com/news/security/240012810/kaspersky-sms-trojans-account-for-over-half-of-smartphone-malware.htm.

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

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

[18] "How to Remove Win 7 Anti-Virus 2012," Viruses2, June 7, 2011, www.2-viruses.com/remove-win-7-anti-virus-2012.

[19] Securelist, "Spam in October 2012," November 23, 2012, www.securelist.com/en/analysis/204792253/Spam_in_October_2012.

[20] Matthew J. Schwartz, "DDoS Tools Flourish, Give Attackers Many Options," *InformationWeek*, February 9, 2012, www.informationweek.com/security/attacks/ddos-tools-flourish-give-attackers-many/232600497.

[21] Robert McGarvey, "Big Banks Hit with Denial of Service Attacks," *Credit Union Times*, September 20, 2012, www.cutimes.com/2012/09/20/big-banks-hit-with-denial-of-service-attacks.

[22] Stacy Cowly, "Grum Takedown: '50 Percent of Worldwide Spam Is Gone'," *CNN Money*, July 19, 2012, http://money.cnn.com/2012/07/19/technology/grum-spam-botnet/index.htm.

[23] 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.

[24] Securelist, "Spam in October 2012," November 23, 2012, www.securelist.com/en/analysis/204792253/Spam_in_October_2012.

[25] Kevin McCaney, "Spear-Phishing Campaign Targets Gov Addresses Taken in Stratfor Hack," *GCN*, February 16, 2012, http://gcn.com/articles/2012/02/16/stratfor-hack-spear-phishing-feds-military.aspx.

[26] Bill Singer, "The FBI Issues Holiday Warning About Smishing, Vishing and Other Scams by Cyber-Criminals," *Huffington Post*, November 28, 2010, www.huffingtonpost.com/bill-singer/the-fbi-issues-holiday-wa_b_788869.html.

[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] Aramco, "At a Glance," www.saudiaramco.com/en/home.html#our-company%257C%252Fen%252Fhome%252Four-company%252Fat-a-glance.baseajax.html (accessed December 4, 2012).

[29] Taylor Armerding, "Line Blurs Between Insider, Outsider Attacks," *Network World*, October 25, 2012, www.networkworld.com/news/2012/102512-line-blurs-between-insider-outsider-263690.html.

[30] Christopher Williams, "Espionage Virus Sent Blueprints to China," *The Telegraph*, June 21, 2012, www.telegraph.co.uk/technology/news/9346734/Espionage-virus-sent-blueprints-to-China.html.

[31] "MasterCard Warns of Possible Security Breach, Visa Also Reportedly Affected," *FoxNews.com*, March 30, 2012, www.foxnews.com/us/2012/03/30/visa-mastercard-warn-massive-security-breach-report-says.

[32] Taylor Armerding, "Hacktivism Gets Attention, But Not Much Long-Term Change," *CSO Online*, November 29, 2012, www.csoonline.com/article/722694/hacktivism-gets-attention-but-not-much-long-term-change.

[33] Microsoft Corporation, "Microsoft Outlines Evolved Security, Privacy, and Reliability Strategies for Cloud and Big Data," February 28, 2012, www.microsoft.com/en-us/news/press/2012/feb12/02-28MSRSA2012PR.aspx.

[34] Seymour E. Goodman and Herbert S. Lin, "Toward a Safer and More Secure Cyberspace," Committee on Improving Cybersecurity Research in the United States/Computer Science and Telecommunications Board, www.cyber.st.dhs.gov/docs/Toward_a_Safer_and_More_-Secure_Cyberspace-Full_report.pdf (accessed February 20, 2013).

[35] Melanie Pinola, "If Your Router Is Still Using the Default Password, Change It Now!" *IT World*, December 7, 2012, www.itworld.com/consumerization-it/326421/if-your-router-still-using-default-password-change-it-now.

[36] Datasavers, Inc., "Computer and Internet Security," www.datasaversinc.com/computer-and-internet-security (accessed on January 24, 2013).

[37] Matthew J. Schwartz, "Antivirus Tool Fail: Blocking Success Varies by 58%," *InformationWeek*, October 25, 2012, www.informationweek.com/security/antivirus/antivirus-tool-fail-blocking-success-var/240009991.

[38] Department of Homeland Security, "Safeguard and Secure Cyberspace," www.dhs.gov/safeguard-and-secure-cyberspace (accessed December 8, 2012).

[39] Department of Homeland Security, "Safeguard and Secure Cyberspace," www.dhs.gov/safeguard-and-secure-cyberspace (accessed December 8, 2012).

[40] Department of Homeland Security, "Protected Critical Infrastructure Information (PCII) Program," www.dhs.gov/protected-critical-infrastructure-information-pcii-program, 2012).

[41] DreamHost, "DreamHost – About Us," http://dreamhost.com/about-us (accessed December 6, 2012).

[42] Simon Anderson, "Security Update,"DreamHost Updates (blog), January 21, 2012, http://blog.dreamhost.com/2012/01/21/security-update/.

[43] Brad Moon, "Symantec Doing Damage Control Over Hack," *Investor Place*, January 31, 2012, http://investorplace.com/2012/01/symantec-doing-damage-control-over-hack.

[44] Ellen Messmer, "DDoS Attacks Against Banks Raise Question: Is This Cyberwar?" *Network World*, October 24, 2012, www.networkworld.com/news/2012/102412-bank-attacks-cyber-war-263664.html.

[45] SpaFinder, "About Us," www.spafinder.com/about/index.jsp (accessed January 22, 2013).

[46] "Hosting Service Couldn't Protect SpaFinder from Application Layer 4 and Layer 7 DDoS Attacks," www.prolexic.com/knowledge-center-ddos-mitigation-case-studies-spafinder.html (accessed December 12, 2012).

[47] US-CE, "Anonymous DDoS Activity," January 24, 2012, www.us-cert.gov/cas/techalerts/TA12-024A.html.

[48] Quinn Norton, "How Anonymous Got Political," *New Internationalist*, December 1, 2012, www.newint.org/features/2012/12/01/anonymous-into-politics.

[49] "We Are Anonymous, We Are Legion," *Yale Law and Technology*, November 9, 2009, www.yalelawtech.org/anonymity-online-identity/we-are-anonymous-we-are-legion.

[50] Chris Landers, "Serious Business: Anonymous Takes On Scientology (and Doesn't Afraid of Anything)," *Baltimore City Paper*, April 2, 2008.

[51] Quinn Norton, "How Anonymous Got Political," *New Internationalist*, December 1, 2012, www.newint.org/features/2012/12/01/anonymous-into-politics.

[52] Jim Puzzanghera, "Scientology Feud with Its Critics Takes to Internet," *The Los Angeles Times*, February 5, 2008, www.latimes.com/news/local/la-me-scientology5feb05,1,3440284.story.

[53] Shaun Davies, "The Internet Pranksters Who Started a War," *The Australian*, May 8, 2008, http://web.archive.org/web/20080922163556/ http://news.ninemsn.com.au/article.aspx?id=459214.

[54] Sean Ludwig, "10 Things You Need to Know About Anonymous' Stratfor Hack," *VB/News*, December 28, 2011, http://venturebeat.com/2011/12/28/anonymous-stratfor-hack-10-things-to-know.

[55] Natasha Lennard, "Anonymous Takes on Syrian Government," *Salon*, November 30, 2012, www.salon.com/2012/11/30/anonymous_takes_on_syrian_government.

[56] Ben Brumfield, "Anonymous Threatens Justice Department Over Hactivist Death," *CNN*, January 27, 2013, www.cnn.com/2013/01/26/tech/anonymous-threat/index.html.

[57] Hayley Tsukayama, "25 Alleged Anonymous Members Arrested After Interpol Investigation," *Washington Post*, February 29, 2012, http://articles.washingtonpost.com/2012-02-29/business/35444725_1_interpol-web-denial-of-service-attack-service-attacks.

[58] Amanda Holpuch, "Anonymous Collective Will Decline in 2013, McAfee Report Predicts," *The Guardian*, December 28, 2012, www.guardian.co.uk/technology/us-news-blog/2012/dec/28/anonymous-collective-decline-2013-mcafee.

[59] "Anonymous Reacts to Sabu's Betrayal of LulzSec," *Gizmodo*, March 6, 2012, http://gizmodo.com/5890961/anonymous-reacts-to-sabus-betrayal-of-lulzsec.

[60] Michael Wilson, "From Smiling Coffee Vendor to Terror Suspect," *New York Times*, September 25, 2009, www.nytimes.com/2009/09/26/nyregion/26profile.html?_r=1.

[61] Regional Computer Forensics Laboratory, "Regional Computer Forensics Laboratory Annual Report for FY 2009, 5.0 Casework/Investigations," www.rcfl.gov/Downloads/Documents/annual_report_web/annual_05_01_casework_09.html (accessed January 26, 2011).

[62] Department of Justice, "Press Release: Najibullah Zazi Pleads Guilty to Conspiracy to Use Explosives Against Persons or Property in U.S., Conspiracy to Murder Abroad, and Providing Material Support to al Qaeda," Federal Bureau of Investigation of New York, February 22, 2010, http://newyork.fbi.gov/dojpressrel/pressrel10nyfo022210.htm.

[63] NOAA's National Ocean Service, "Incident News: M/V Cosco Busan," Office of Response and Restoration, November 7, 2007, www.incidentnews/gov/incident/7708.

[64] International Bird Rescue Research Center, "Dark Days on San Francisco Bay," www.ibrrc.org/Cosco_Busan_spill_2007.htm (accessed January 27, 2011).

[65] "Oil Spill Captain Gets Prison Sentence," *San Francisco Bay Crossings*, January 27, 2011.

[66] Regional Computer Forensics Laboratory, "Fleet Mgt. Ltd. Agrees to Pay $10 Million for Pollution and Obstruction Crimes," August 19, 2009, www.rcfl.gov/index.cfn?fuseAction=Public.N_SV004.

[67] "Oil Spill Captain Gets Prison Sentence," *San Francisco Bay Crossings*, January 27, 2011.

[68] Department of Justice, "Press Release: Cosco Busan Operator Admits Guilt in Causing Oil Spill," Office of Public Affairs, August 13, 2009, www.justice.gov/opa/pr/2009/August/09-enrd-797.html.

[69] Minnesota Lawyers, "Divorce and Computer Forensics," www.nvo.com/beaulier/divorceand-forensicevidence (accessed January 27, 2011).

[70] "Daniel Shana Threatens To Inflict 'Columbine Take 2' On Lynn University Students," *Huffington Post*, November 19, 2010, www.huffingtonpost.com/2010/11/19/Daniel-shana-threatens-to_n_786015.html.

[71] "Man Charged with Columbine-Type Plot," *MyFoxBoston*, November 18, 2010, www.myfoxboston.com/dpp/news/crime_files/crime_watch/man-charged-with-columbine-style-plot-20101118.

[72] Bureau of Labor Statistics, "Private Detectives and Investigators," Occupational Outlook Handbook, 2010-11 Edition, www.blos.gov/oco/ocos157.htm (accessed January 27, 2011).

[73] Bureau of Labor Statistics, "Private Detectives and Investigators," Occupational Outlook Handbook, 2010-11 Edition, www.blos.gov/oco/ocos157.htm (accessed January 27, 2011).

[74] "Computer Forensic Investigator: High-tech Career in Law Enforcement," *Hub Pages*, http://hubpages.com/hub/Computer-Forensic-Investigator-High-tech-Career-in-Law-Enforcement (accessed January 27, 2011).

[75] Bureau of Labor Statistics, U.S. Department of Labor, *Occupational Outlook Handbook*, 2012-13 Edition, Private Detectives and Investigators, www.bls.gov/ooh/protective-service/private-detectives-and-investigators.htm (accessed January 24, 2013).

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

VIGNETTE

What Is the National Security Agency (NSA) Up To?

The National Security Agency (NSA), an intelligence agency of the U.S. government, is responsible for the making and breaking of codes used to encrypt sensitive communications, and for the interception of signals on behalf of the federal government. The information generated and intercepted by the NSA is used for intelligence and counterintelligence purposes and to support U.S. military operations.

The NSA has established a comprehensive telecommunications network capable of monitoring billions of emails and phone calls—whether they originate within the United States or overseas. AT&T's powerful ground-based communications stations, which are used to relay messages to communications satellites, are a major component of the NSA network; that includes three 105-foot dishes in rural Pennsylvania that relay most U.S. communications to and from Europe and the Middle East and three similar dishes in California that handle communications for the Pacific Rim and Asia.[1] It has been estimated that the NSA also has anywhere from ten to twenty secret listening posts,

which the agency can use to tap into the telecommunications switches of other U.S. telecom carriers to capture domestic traffic traveling over these networks.

The Advanced Encryption Standard (AES) algorithm is the current state-of-the-art standard for encrypting top-secret communications. According to experts, it would take approximately 12 billion years to break this code via a trial-and-error brute force attack using today's supercomputers. However, in recent years, the NSA has made vast breakthroughs in its ability to crack codes. The agency is employing advanced technology to build super-fast computers and sophisticated software "capable of breaking the AES encryption key within an actionable time period."[2] Such research has been going on since at least 2004 at a computer research center in Oak Ridge, Tennessee, where the goal is to build a supercomputer that can operate at phenomenal rate of 10^{18} operations per second.[3]

Once an encrypted message is broken, software created by a company called Narus, part of Boeing, searches it for target addresses, locations, countries, and phone numbers, as well as certain names, keywords, and phrases on NSA's watch list. Suspicious communications are recorded and then transmitted to other locations where it can be stored and, if need be, accessed by NSA code breakers, data miners, intelligence analysts, counterterrorism specialists, and others. One of those locations is a new $1.5 billion, one million square foot data center located in Utah. It boasts a prodigious data storage capacity measured in units of yottabytes (10^{24} bytes).[4] This is more than enough capacity to store the current global volume of all Internet traffic for a thousand years.[5]

By law, NSA's intelligence gathering is limited to the interception of foreign communications. Intelligence activities involving U.S. citizens and activities conducted within the United States require special consideration because those activities could violate privacy rights and civil liberties guaranteed under the Fourth Amendment and other laws. Various advocacy groups, including the American

Civil Liberties (ACLU), the Center for Democracy and Technology (CDT), and the Electronic Frontier Foundation (EFF), have expressed concern that government agencies, including the NSA, are conducting extensive surveillance of both foreign nationals and millions of Americans.[6]

In early 2012, NSA chief General Keith Alexander testified in front of the House Armed Services subcommittee on Emerging Threats and Capabilities and denied that the NSA had the capability to monitor, inside the United States, Americans' text messages, phone calls, and emails.[7] However, the NSA has not always been entirely forthcoming about its activities. In late 2005, an article in the *New York Times* revealed that President George W. Bush had secretly authorized the NSA to conduct warrantless eavesdropping on thousands of Americans beginning in 2002.[8,9,10]

Questions to Consider

1. What potential issues are raised if the U.S. government is indeed eavesdropping on the communications of its citizens?
2. What privacy rights and civil liberties would such action violate?

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. Why and how are employers increasingly using workplace monitoring?
5. 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. 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.

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, while also developing a better understanding of the developments in information technology that could impact this right. The chapter 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 United States 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 United States 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** is 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. 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."[11]

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."[12] 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 its use).[13] 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 Web site (*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 this personal financial data carries a high risk of loss of privacy and potential financial loss. Individuals should be concerned about how this personal data is protected by businesses and other organizations and whether or not it is shared with other people or companies.

Fair Credit Reporting Act (1970)

The **Fair Credit Reporting Act** 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 check those 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 is retained. It also prohibits the credit-reporting bureau from giving out information about you to your employer or potential employer without your written consent.[14]

Right to Financial Privacy Act (1978)

The **Right to Financial Privacy Act** protects the records of financial institution customers from unauthorized scrutiny by the federal government. Prior to 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 their 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), 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.[15] 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 is gathered, with whom that data is shared, how the data is used, and how the data is 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 a company's privacy policy is changed, customers 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. 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, to other financial institutions.
- *Safeguards Rule*—This rule requires each financial institution to document a data security plan describing the company's 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 such means 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** 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.[16]

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.

Health Insurance Portability and Accountability Act (1996)

The **Health Insurance Portability and Accountability Act (HIPAA)** 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.[17] 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 in 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.

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. Those who misuse data may be fined $250,000 and serve up to 10 years in prison. 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.

Illustrating how difficult it is for healthcare companies to adhere to HIPAA regulations is the case of an employee of a staffing agency filling in at a hospital in Mission Hills, California. The employee, apparently unaware of HIPAA privacy regulations, posted a patient's medical record, including her full name, to his Facebook page. He also added a comment stating the reason for her admission and making fun of her condition. Several

people commented on the Facebook post, noting that what the individual had done violated HIPAA laws. The employee responded that his posting was just a joke, and expressed surprise that people were upset.[18]

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.[19] In a move many feel was designed to spur other small practices into action, the OCR investigated a five-physician practice in Phoenix for posting its surgery and appointment schedules on the Internet over a several year period. This posting was deemed to be a HIPAA violation and the practice was required to pay a $100,000 fine and take corrective actions.[20]

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 will instead increase costs and paperwork for doctors without improving medical care. All agree that the medical industry must make a substantial investment to achieve compliance.

The American Recovery and Reinvestment Act (2009)

The **American Recovery and Reinvestment Act** 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, including banning the sale of health information, promoting the use of audit trails and encryption, and providing rights of access for patients.

Children's Personal Data

According to the Center for Media Research, teens spend over five hours per week surfing the Web, and over 40 percent of them claim that their parents have no idea what they are looking at online. Meanwhile, Norton Online Living reports that 40 percent of teens have received an online request for personal information. In addition, an estimated 16 percent of U.S. children have been approached online by a stranger.[21]

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)** 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 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.[22]

Children's Online Privacy Protection Act (1998)

According to the **Children's Online Privacy Protection Act (COPPA)**, any Web site 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.

Artist Arena operates online fan clubs for pop stars such as Demi Lovato, Justin Bieber, Rihanna, Selena Gomez, and other singers popular with preteens. In October 2012, the Federal Trade Commission accused the company of collecting personal information—such as names, addresses, and birth dates—from over 100,000 preteens who visited these sites. Rather than argue its guilt or innocence, Artist Arena proposed a settlement in which it would pay $1 million and delete any information it may have collected in violation of COPPA to settle the alleged wrong doing.[23]

Electronic Surveillance

This section covers laws that address government surveillance, including various forms of electronic surveillance. New laws have been added and old laws amended in recent years

in reaction to worldwide terrorist activities and the development of new communication technologies.

Communications Act (1934)
The **Communications Act** established the Federal Communications Commission and gave it responsibility for regulating all non-federal-government use of radio and television broadcasting and all interstate telecommunications as well as all international communications that originate or terminate in the United States. The act also restricted the government's ability to secretly intercept communications.

The Foreign Intelligence Surveillance Act (FISA) (1978)
The **Foreign Intelligence Surveillance Act (FISA)** 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."[24] 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.

The act also created the **Foreign Intelligence Surveillance Act (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.[25] In 2011, the Department of Justice submitted 1,745 applications for electronic surveillance to the FISA court, and none of those applications were denied.[26]

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, 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."[27]

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."[28] 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. In 2011, federal judges authorized 792 wiretaps and state judges authorized 1,940 wiretaps. These led to the arrest of more than 3,547 people and 465 convictions. Two wiretap requests were rejected.[29] These numbers only include statistics from the 25 states that reported data and do not include wiretap orders in terrorism investigations, which are authorized by the Foreign Intelligence Surveillance Act 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.

Electronic Communications Privacy Act (1986)

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. 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 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, instant 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.

A 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).[30]

Communications Assistance for Law Enforcement Act (1994)

The **Communications Assistance for Law Enforcement Act (CALEA)** 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. The 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.[31]

A provision in the act covering radio-based data communication grew from a realization that the Electronic Communications Privacy Act 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) of 2001 was passed just 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. 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. Table 4-1 summarizes the key provisions of the USA PATRIOT Act as they affect the privacy of individuals.

TABLE 4-1 Key provisions of the USA PATRIOT Act

Section	Issue addressed	Summary
201	Wiretapping in terrorism cases	Added several crimes for which federal courts may authorize wiretapping of people's communications
202	Wiretapping in computer fraud and felony abuse cases	Added computer fraud and abuse to the list of crimes for which the FBI may obtain a court order to investigate under Title III of the Wiretap Act
203(b)	Sharing wiretap information	Allows the FBI to disclose evidence obtained under Title III to other federal officials, including "law enforcement, intelligence, protective, immigration, national defense, [and] national security" officials
203(d)	Sharing foreign intelligence information	Provides for disclosure of threat information obtained during criminal investigations to "appropriate" federal, state, local, or foreign government officials for the purpose of responding to the threat
204	FISA pen-register/ trap-and-trace exceptions	Exempts foreign intelligence surveillance from statutory prohibitions against the use of pen-register or trap-and-trace devices, which capture "addressing" information about the sender and recipient of a communication; it also exempts the U.S. government from general prohibitions against intercepting electronic communications and allows stored voice-mail communication to be obtained by the government through a search warrant rather than more stringent wiretap orders
206	FISA roving wiretaps	Expands FISA to permit "roving wiretap" authority, which allows the FBI to intercept any communications to or by an intelligence target without specifying the telephone line, computer, or other facility to be monitored
207	Duration of FISA surveillance of non-U.S. agents of a foreign power	Extends the duration of FISA wiretap orders relating to an agent of a foreign power from 90 days to 120 days, and allows an extension in 1-year intervals instead of 90-day increments
209	Seizure of voice-mail messages pursuant to warrants	Enables the government to obtain voice-mail messages under Title III using just a search warrant rather than a wiretap order, which is more difficult to obtain; messages stored on an answering machine, however, remain outside the scope of this section

(Continued)

TABLE 4-1 Key provisions of the USA PATRIOT Act *(Continued)*

Section	Issue addressed	Summary
212	Emergency disclosure of electronic surveillance	Permits providers of communication services (such as telephone companies and Internet service providers) to disclose consumer records to the FBI if they believe immediate danger of serious physical injury is involved; communication providers cannot be sued for such disclosure
214	FISA pen-register/ trap-and-trace authority	Allows the government to obtain a pen-register/trap-and-trace device "for any investigation to gather foreign intelligence information"; it prohibits the use of FISA pen-register/ trap-and-trace surveillance against a U.S. citizen when the investigation is conducted solely on the basis of activities protected by the First Amendment
215	FISA access to tangible items	Permits the FBI to compel production of any record or item without showing probable cause; people served with a search warrant issued under FISA rules may not disclose, under penalty of law, the existence of the warrant or the fact that records were provided to the government. It prohibits investigation of a U.S. citizen when it is conducted solely on the basis of activities protected by the First Amendment.
217	Interception of computer-trespasser communications	Creates a new exception to Title III that permits the government to intercept the "communications of a computer trespasser" if the owner or operator of a "protected computer" authorizes it; it defines a protected computer as any computer "used in interstate or foreign commerce or communication" (because of the Internet, this effectively includes most computers)
218	Purpose for FISA orders	Expands the application of FISA to situations in which foreign intelligence gathering is merely a significant purpose rather than the sole purpose
220	Nationwide service of search warrants for electronic evidence	Expands the geographic scope in which the FBI can obtain search warrants or court orders for electronic communications and customer records
223	Civil liability and discipline for privacy violations	Provides that people can sue the government for unauthorized disclosure of information obtained through surveillance
225	Provider immunity for FISA wiretap assistance	Provides immunity from lawsuits for people who disclose information to the government pursuant to a FISA wiretap order, a physical search order, or an emergency wiretap or search
505	Use of National Security Letters (NSLs) to gain access to personal records	Authorizes the attorney general or a delegate to compel holders of your personal records to turn them over to the government simply by writing an NSL, which is not subject to judicial review or oversight; NSLs can be used against anyone, including U.S. citizens, even if they are not suspected of espionage or criminal activity

Source Line: "Key Provisions of USA Patriot Act," NewsMax.com, ©December 22, 2005, http://archive.newsmax.com/archives/articles/2005/12/22/113858.shtml.

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. During 2011, the FBI issued 16,511 NSL requests for information pertaining to 7,201 U.S. persons.[32] The 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.[33]

Foreign Intelligence Surveillance Act Amendments Act (2008)

A few months after the September 11, 2001 terrorist attacks, President George W. Bush signed a presidential 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. The Bush administration and other advocates of the program argued that it 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 Central Intelligence Agency (CIA) overseas operations. Warrants were still required for eavesdropping on strictly domestic U.S. communications, say, phone calls from someone in Atlanta to a person in Los Angeles.[34] The disclosure of this secret program triggered three years of heated Congressional debate that ended with Congress passing the **Foreign Intelligence Surveillance Act (FISA) Amendments Act** in 2008 granting NSA expanded authority to collect, without court-approved warrants, international communications as they flow through U.S. telecom network equipment and facilities. The targets of the warrantless eavesdropping had to be "reasonably believed" to be outside the United States, while 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).[35]

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.[36]

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

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.

Organisation for Economic Co-operation and Development Guidelines 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 34 member countries, including Australia, Canada, France, Germany, Italy, Japan, Mexico, New Zealand, 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.[37]

The OECD's fair information practices, established in 1980, are often held up as the model of ethical treatment of consumer data. These guidelines are composed of the eight principles summarized in Table 4-2. The OECD guidelines were nonbinding and as a result data privacy laws still varied widely across Europe.[38]

TABLE 4-2 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 is 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 Line: Organisation for Economic Co-operation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," www.oecd.org/document/18/0,3343,en_2649_34255_18151861111,00.html.

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 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-European Union (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.[39]

The following list summarizes the basic tenets of the directive:

- *Notice*—An individual has the right to know if his or her personal data is 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 its 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.[40]

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 European Union; only U.S. companies that are certified as meeting safe harbor principles are 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 also are certified.[41]

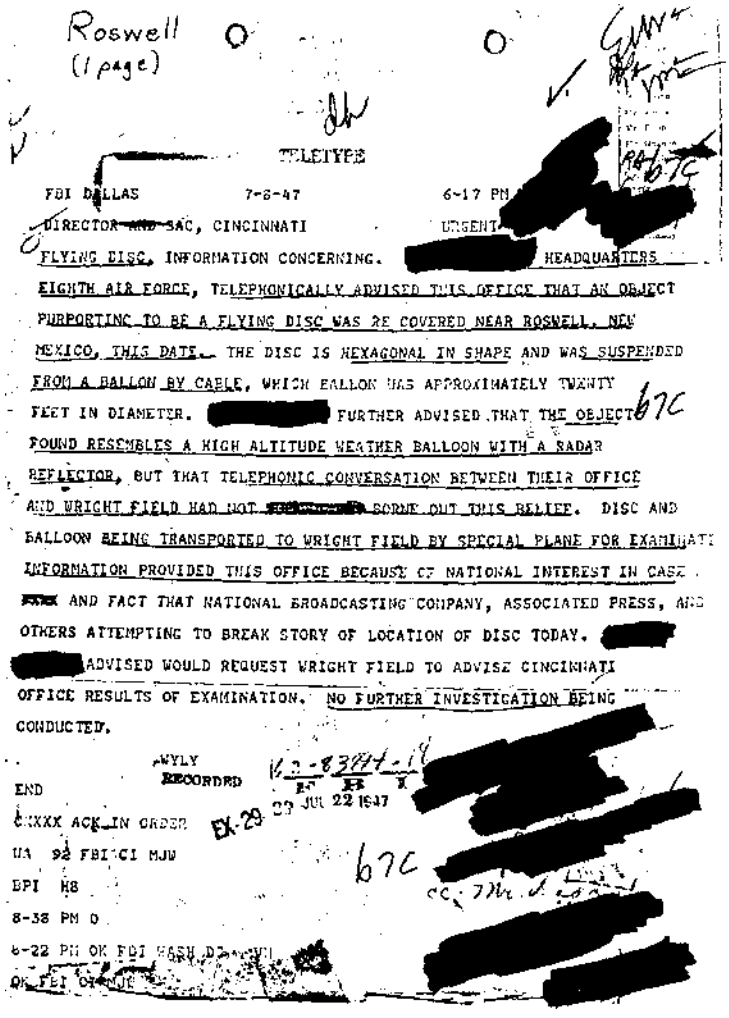
In 2012, the European Commission proposed a new **European Data Protection Regulation** to replace the 1995 Data Protection Directive. The original directive was implemented at a time when less that 1 percent of Europeans used the Internet;[42] e-commerce was in its infancy; and Google, cloud computing, social networks, cell phones, and smart cards had not been invented. Few had even envisioned the changes the Internet would bring. The original 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. 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 proposed regulation would simplify matters by enforcing a single set of rules for data protection across the EU. This would eliminate the need for costly administrative processes and save countries an estimated €2.3 billion (about $3.03 billion USD) per year.[43] However, the new regulation has yet to be approved.

Access to Government Records

The government has a great capacity to store data about each and every one of us and about the proceedings of its various organizations. The Freedom of Information Act 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 recordkeeping systems.

Freedom of Information Act (FOIA) (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 4-1). Notice that much of the information has been redacted, a practice common with FOIA requests.



Roswell
(1 page)

TELETYPE

FBI DALLAS 7-8-47 6-17 PM

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 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.

WYLY
RECORDED
62-83844-14
EX-29
22 JUL 22 1947

END

XXXX ACK IN ORDER

UA 92 FBI CI MJW

BPI H8

8-38 PM O

6-22 PM OK FBI WASH D.C. WI

OK FBI CINCIN

67C

cc: [redacted]

FIGURE 4-1 Response to FOIA request for information about the 1947 Roswell incident
Source Line: http://vault.fbi.gov/Roswell UFO/Roswell UFO Part 1 of 1/view

The act is often used by whistleblowers 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 several hundred dollars 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.[44]

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 the request 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 2011, there were 644,165 FOIA requests for government data—with 30,369 requests declined and a backlog of 83,490 requests.[45]

Exemptions to the FOIA bar disclosure of information that could compromise national security or interfere with an active law enforcement investigation. Another exemption prevents disclosure of records if it would invade someone's privacy. In this case, a balancing test is applied to evaluate whether the privacy interests at stake are outweighed by competing public interests.

The use of the FOIA to access information can lead to a dispute between those who feel it is important to reveal certain information and those who feel certain government data should not be made public, including, in some cases, those whose privacy is being impacted. For example, in response to the December 2012 school shootings in Newtown, Connecticut, *The Journal News*, a newspaper serving southern New York state, created an interactive map of legal gun owners. The newspaper thought it was providing a useful service to its subscribers by enabling users to zoom in on the interactive map to see the names and addresses of all firearm permit holders in Westchester and Rockland counties, including judges, law enforcement officers, and federal agents. The data used to create the map was obtained legally through a Freedom of Information Act request made to county government offices.[46] After the article ran, some gun owners expressed concern that they were now at increased risk of theft by criminals seeking weapons to commit future crimes. Meanwhile, some non-gun-owners expressed the concern that criminals would now know which homes they could target without fear of getting shot. In response, a blogger posted the names, home addresses, and phone numbers of *Journal News* staff members—as well as any other public information he could find—on his blog in retaliation for what he felt was harassment of gun owners.[47]

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 issues that address 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.[48]

In a case involving the Privacy Act, a woman and her young daughter, both U.S. citizens, reentered the country from Canada border. A customs database incorrectly branded the mother as "armed and dangerous." She was then handcuffed, questioned for several hours, and finally released without explanation. The woman sued under the Privacy Act and sought damages from the Department of Homeland Security for the agency's failure to ensure the accuracy of its computer records. A federal appeals court held that the Privacy Act provides monetary damages for harms stemming from inaccurate government records.[49]

KEY PRIVACY AND ANONYMITY ISSUES

The rest of this chapter discusses a number of current and important privacy issues, including data breaches, electronic discovery, consumer profiling, workplace monitoring, and advanced surveillance technology.

Data Breaches

An alarming number of identity theft incidents can be traced back to data breaches involving large databases of personal information. Data breaches are sometimes caused by hackers breaking into a database, but more often than one might suspect, they are caused by carelessness or failure to follow proper security procedures. For example, a laptop computer containing the unencrypted names, birth dates, and Social Security numbers of 26.5 million U.S. veterans was stolen from the home of a Veterans Affairs (VA) analyst. The analyst violated existing VA policy by removing the data from his workplace.[50]

Table 4-3 identifies the eight largest U.S. data breaches.

The number of data breach incidents is alarming (over 1,450 in 2012 alone),[51] as is the lack of initiative by some companies in informing the people whose data was stolen. Organizations are reluctant to announce data breaches due to the ensuing bad publicity and potential for lawsuits by angry customers. However, victims whose personal data was compromised during a data breach need to be informed so that they can take protective measures.

As mentioned earlier in this chapter, the Health Information Technology for Economic and Clinical Health Act included strong privacy provisions for electronic health records.

TABLE 4-3 Largest reported U.S. data breaches

Date incident was reported	Number of records involved	Organization(s) involved
March 17, 2012	150 million	Shanghai Roadway D&B Marketing Services, Ltd.
January 20, 2009	130 million	Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank
January 17, 2007	94 million	The TJX Companies
June 1, 1984	90 million	TRW, Sears Roebuck
April 26, 2011	77 million	Sony Corporation
June 19, 2005	40 million	CardSystems, Visa, MasterCard, American Express
December 26, 2011	40 million	Tianya
July 28, 2011	35 million	SK Communications, Nate, Cyworld

Source Line: Open Security Foundation's DataLossDB, http://datalossdb.org.

One such mandate is that within 60 days after discovery of a data breach, each individual whose health information has been exposed must be notified, and if a breach involves 500 or more people, notice must be provided to prominent media outlets.[52] According to the Health Information Trust Alliance, from 2009 to mid-2012, there were 495 medical data breaches involving 21 million patient records. The average time to notify individuals following a breach was 68 days, with over half of the organizations failing to notify affected individuals within the 60-day deadline.[53]

Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring organizations to disclose security breaches involving personal information.[54] Some states have extremely stringent laws regarding the reporting of a data breach of patient health records. For example, under California law, a data breach involving protected health information must be reported to government agencies and affected individuals within five days of discovery. The Lucile Packard Children's Hospital at Stanford University was fined $250,000 by the California Department of Public Health when it took 19 days to report the theft of a computer with protected health information on 532 patients.[55]

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.

Zappos, an online shoe and clothing retailer and a subsidiary of Amazon, was subject to a major data breach wherein a cybercriminal gained access to customer names, email addresses, billing and shipping addresses, phone numbers, the last four digits of their credit card numbers, and the customers' encrypted passwords for the Zappos Web site. The database that stores credit card and payment data for the company was not breached. Zappos immediately emailed its 24 million customers to notify them of the data breach

and to strongly suggest that they reset their password on Zappos.com and any other Web site where they used a similar password.[56] Despite what many observers considered to be a timely response to the incident, Amazon and Zappos were hit with nine federal class action lawsuits within three months of the incident. Plaintiffs said they feared an increased risk of identity theft and other financial-related crimes.[57] It is likely that Zappos faces millions of dollars in legal fees and perhaps tens of millions of dollars in additional costs to settle the claims.

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 will 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 electronic 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, in what format data will be provided, and whether production of certain electronically stored information 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, what topics and/or individuals need to be included in the e-discovery process, etc.).

Often organizations will send a litigation hold 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. Apple and Samsung were embroiled in a long-running dispute involving alleged patent infringement. During the 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.[58]

It can require extensive time to collect, prepare, and review the tremendous volume of ESI kept by an organization. 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.[59]

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 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

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?

Consumer Profiling

Companies openly collect personal information about users when they register at Web sites, complete surveys, fill out forms, or enter contests online. Many companies also obtain information about Web surfers through the use of **cookies**—text files that can be downloaded to the hard drives of users who visit a Web site, so that the Web site is able to identify visitors on subsequent visits. Companies also use tracking software to allow their Web sites 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 Web site 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.

In early 2012, members of the Obama administration, digital advertisers, browser software manufacturers, and privacy advocates agreed in principle to create a "Do Not Track" button for Web browsers. The idea was to make it easy for Internet users to communicate their desire to not be tracked as they surfed the Web. Users of the Firefox, Explorer, or Safari Web browsers can select a "Do Not Track" option so that the browser sends a message to each site visited that you do not wish to have cookies deposited on your computer. However, it is up to each individual Web site to decide if they will comply with your request to not be tracked; they are not required to honor your request.[60]

Outside of the Web environment, 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, orders from a mail-order catalog, or registers a car with the DMV, the data is 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 this 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 this data is 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 individual Web surfers who visit their sites. Data gathered about a user's Web browsing through the use of cookies is anonymous, as long as the network advertiser doesn't link the data with personal information. However, if a Web site visitor volunteers personal information, a Web site 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 this information becomes extremely valuable to the Web site operator, who is trying to build a relationship with Web site visitors and turn them into customers. The operator can use this data to initiate contact or sell it to other organizations with which they have marketing agreements.

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.

Opponents of consumer profiling are also concerned that personal data is being gathered and sold to other companies without the permission of consumers who provide the data. After the data has been collected, consumers have no way of knowing how it is used or who is using it.

Workplace Monitoring

Plenty of data exists to support the conclusion that many workers waste large portions of their work time doing non-work-related activity. One recent study revealed that between 60 to 80 percent of workers' time online has nothing to do with work.[61] Another source estimates that, on average, workers spend about four or five hours per week on personal matters. In a recent survey by an IT staffing firm, 54 percent of companies reported they were banning the use of social networking sites such as Facebook, Twitter, MySpace, and LinkedIn to help reduce waste at work.[62] As discussed in Chapter 2, many organizations have developed policies on the use of IT in the workplace in order to protect against employee 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 sex, race, or national origin can also spawn lawsuits.) The institution and communication of an IT usage policy establishes boundaries of acceptable behavior and enables 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. Many U.S. firms find it necessary 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, Internet use, and files on company computers were not private and that their use might be monitored.

Society is 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, many 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.

The U.S. Food and Drug Administration admitted in 2012 that it monitored the private email accounts of nine of its scientists and doctors who had expressed concerns about the FDA process for approving medical devices. Through the use of keystroke monitoring

software, the FDA process captured some 80,000 pages of email including users' email passwords and bank account information. The FDA sends a mixed signal to employees by telling them that their email may be monitored, while at the same time telling them that the use of their government-issued computers for limited personal use is acceptable. Such a message could be interpreted as setting a reasonable expectation of privacy.[63] The impacted employees filed a lawsuit claiming that FDA officials violated their privacy and constitutional rights by monitoring their private email communications. Some investigators believe that the FDA used the emails to build a case to retaliate against the employees.[64]

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 suggests 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 4.2 million closed circuit TV cameras (CCTV) in operation throughout Great Britain—which amounts to 1 CCTV camera for every 14 people. China, by way of comparison, has 2.75 million cameras, or 1 camera for every 472,000 citizens.[65] The number of cameras in London was greatly expanded during the 2012 Olympics, and a system called DYVINE enables all London CCTV cameras to be monitored and controlled from the New Scotland Yard.[66]

Washington, D.C.'s Homeland Security and Emergency Management Agency (HSEMA) receives video feeds from more than 4,500 surveillance cameras embedded in and around its schools and public transportation system hubs. HSEMA is evaluating the addition of thousands of more video feeds from private businesses such as banks, corner stores, and gas stations around the city. According to an HSEMA spokesperson, the cameras are designed to raise "situational awareness" during "developing significant events."[67]

The Chicago Transit Authority (CTA) has installed 17,000 cameras in an attempt to reduce crime on their system. According to the CTA, during the first ten months of 2012,

the cameras aided in the arrest of 135 criminals and helped reduce the overall crime rate on the CTA system by 23 percent.[68]

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 3,000 surveillance cameras and 2,600 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.[69] 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."[70]

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.[71] 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. This 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 has been ruled as admissible and reliable in court hearings, and there are cases in which such data has had a significant impact on the findings of the court.[72] 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.[73]

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 remains 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 Web site 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.[74] 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.[75]

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 software over the Internet. (Some users 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.

The Senate Judiciary Committee has approved a bill that would extend the criminal and civil liabilities for the improper use of stalking apps to include the software companies that sell them. Such companies would have to disclose the existence of the stalking app on the phone and gain the phone owner's permission before capturing location information and sharing it with anyone else. The proposed bill includes an exception to the permission requirement for parents who want to place tracking software on the cell phones of minor children without them being aware that it is there.[76]

Summary

- 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.
- Few laws provide privacy protection from private industry.
- 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 Gramm-Leach-Bliley Act (GLBA) establishes guidelines for the collection and disclosure of personal financial information; requires financial institutions to document their data security plan; 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 from each of the three consumer credit reporting agencies.
- The Health Insurance Portability and Accountability Act (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 related to the use of electronic health records, 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 Family Educational Rights and Privacy Act (FERPA) provides students with specific rights regarding the release of their student records.
- The Children's Online Privacy Protection Act (COPPA) requires Web sites 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.
- The Communications Act of 1934 established the Federal Communications Commission and gave it responsibility for regulating all non-federal-government use of radio, television, and interstate telecommunications as well as all international communications that originate or terminate in the United States.

- The Foreign Intelligence Surveillance Act (FISA) describes procedures for the electronic surveillance and collection of foreign intelligence information between foreign powers and agents of foreign powers.
- 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 Amendments Act granted the NSA expanded authority to collect, without court-approved warrants, international communications as they flow through U.S. telecommunications networks and equipment.
- The Electronic Communications Privacy Act (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 Communications Assistance for Law Enforcement Act (CALEA) required 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.
- 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 guidelines and call them by different names.
- The Organisation for Economic Co-operation and Development (OECD) 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-European Union 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 European Union.
- The Freedom of Information Act (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.
- The number of data breaches is alarming, as is the lack of initiative by some companies in informing the people whose data is stolen. A number of states have passed data breach notifications laws that require companies to notify affected customers on a timely basis.
- 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.

- Companies use many different methods to collect personal data about visitors to their Web sites, 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.
- Many organizations have developed IT usage policies to protect against employee abuses that can reduce worker productivity and expose employers to harassment lawsuits.
- Many U.S. firms record and review employee communications and activities on the job, including phone calls, email, Web surfing, and computer files.
- 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.
- 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. 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 Web site visited on that phone.

Key Terms

American Recovery and Reinvestment Act
Bill of Rights
Children's Online Privacy Protection Act (COPPA)
cookie
Communications Act of 1934
Communications Assistance for Law Enforcement Act (CALEA)
Electronic Communications Privacy Act (ECPA)
electronic discovery (e-discovery)
electronically stored information (ESI)
European Data Protection Regulation
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)
foreign intelligence
Foreign Intelligence Surveillance Act (FISA)
Foreign Intelligence Surveillance Act Amendments Act
Foreign Intelligence Surveillance Act Court
Fourth Amendment
Freedom of Information Act (FOIA)
Gramm-Leach-Bliley Act (GLBA)
Health Insurance Portability and Accountability Act (HIPAA)
information privacy
National Security Letter (NSL)
NSL gag provision
opt in
opt out
pen register
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
USA PATRIOT Act
vehicle event data recorder (EDR)
Wiretap Act

Self-Assessment Questions

The answers to the Self-Assessment Questions can be found in Appendix B.

1. The purpose of the Bill of Rights was to:
   a. grant additional powers to the federal government
   b. identify exceptions to specific portions of the Constitution
   c. identify additional rights of individuals
   d. identify requirements for being a "good" U.S. citizen
2. _____ is part of the pretrial phase of a lawsuit in which each party can obtain evidence from the other part by various means.
3. Like many other countries, the United States has developed a single, overarching national data privacy policy. True or False?
4. The _____ Act is enforced by the FTC and is designed to ensure the accuracy, fairness, and privacy of information in the files of credit-reporting companies and to check those systems that gather and sell information about people:
   a. Gramm-Leach-Bliley
   b. Fair Credit Reporting
   c. HIPAA
   d. USA PATRIOT
5. The Fair and Accurate Credit Transactions Act allows consumers to request and obtain a free credit report once each year from each of the three primary consumer credit reporting companies. True or False?
6. Under the provisions of _____, healthcare providers must obtain written consent from patients prior to disclosing any information in their medical records.
7. According to the Children's Online Privacy Protection Act, a Web site that caters to children must:
   a. offer comprehensive privacy policies
   b. notify parents or guardians about its data collection practices
   c. receive parental consent before collecting any personal information from preteens
   d. all of the above
8. _____ is a federal law that assigns certain rights to parents regarding their children's educational records.

9. _____ *v. United States* is a famous court ruling that helped form the basis for the requirement that there be a reasonable expectation of privacy for the Fourth Amendment to apply.
10. The _____ Act describes procedures for the electronic surveillance and collection of foreign intelligence information in communications 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.
11. Which of the following identifies the numbers dialed for outgoing calls?
    a. pen register
    b. wiretap
    c. trap and trace
    d. all of the above
12. In 2011, the Department of Justice submitted 1,745 applications for electronic surveillance to the FISA court and none of those applications were denied. True or False?
13. The _____ Act gave sweeping new powers both to domestic law enforcement and U.S. international intelligence agencies, including increasing the ability of law enforcement to search telephone, email, medical, financial, and other records.
14. The European philosophy of addressing privacy concerns employs strict government regulation, including enforcement by a set of commissioners; it differs greatly from the U.S. philosophy of having no federal privacy policy. True or False?
15. _____ is a term for a set of guidelines that govern the collection and use of personal data.
16. Nearly half the cost of a data breach is a result of lost business opportunity associated with customers whose patronage is lost due to the incident. True or False?
17. A(n) _____ is a text file that a Web site can download to a visitor's hard drive to identify visitors on subsequent visits.
18. The agency that is responsible for protecting the privacy of U.S. consumers is the:
    a. FBI
    b. SEC
    c. Department of Homeland Security
    d. FTC

Discussion Questions

1. Do you think *The Journal News* was justified in publishing the names and addresses of registered gun owners? An FOIA exemption prevents disclosure of records if it would invade someone's personal privacy. Is this an example in which a person's privacy interests are clearly outweighed by competing public interests. Why or why not?

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 the proper and appropriate way to protect the United States from further terrorist acts.
3. Go to the Web site 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 Web site and credit report to find out how can you dispute any information which you believe is in error.
4. Are surveillance cameras worth the cost in terms of resources and loss of privacy, given the role that they play in deterring or solving crimes?
5. The use of National Security Letters by the FBI is highly controversial and has been challenged in court several times. These lawsuits are in various stages of hearings and appeals. Why do you think the use of NSL has been challenged in court so many times? Do research to document the status of the NSL gag provision.
6. Briefly 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?
7. Do research to find out the current status of "Do Not Track," and write a two- to three-paragraph paper summarizing your findings.
8. What is a pen register? What is required in order for a law enforcement agency to gain approve for a pen register?
9. Summarize the Fourth Amendment to the U.S. Constitution. Does it apply to the actions of a publicly held company toward its employees?
10. Do you feel that information systems to fight terrorism should be developed and used even if they infringe on privacy rights or violate the Privacy Act and other such statutes?
11. Why do employers monitor workers? Do you think they should be able to do so? Why or why not?
12. 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?
13. 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. 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?
2. 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. He states that the reason for his request is that there have been an increasing number of complaints about the slowness of email services. In addition, he says he 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?

3. 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?
4. You are a member of a privacy advocacy group. You have been assigned to speak to the board of directors at a major Web advertising firm to help persuade them to support the "Do Not Track" proposal. How would you prepare for this task? What key points would you make?
5. Your friend is considering using an online service to identify people with compatible personalities and attractive physical features who would be interesting to date. Your friend must first submit some basic personal information, then complete a five-page personality survey, and finally provide several recent photos. Would you advise your friend to do this? Why or why not?
6. You have been asked to review how well your company is prepared for a major data breach of your firm's customer database containing some 15 million records with names, addresses, passwords, credit card numbers, and payment history. The goal is to minimize the potential impact of a hacker getting access to this data and to avoid expensive class action lawsuits from affected customers. How would you proceed with this audit? What sort of measures would you look for or recommend?
7. You are a new brand manager for a product line of Coach purses. You are considering purchasing customer data from a company that sells a large variety of women's products online. In addition to providing a list of names, mailing addresses, and email addresses, the data includes an estimate of customers' annual income based on the zip code in which they live, census data, and highest level of education achieved. You could use the data to identify likely purchasers of your high-end purses, and you could then send those people emails announcing the new product line and touting its many features. List the advantages and disadvantages of such a marketing strategy. Would you recommend this means of promotion in this instance? Why or why not?
8. Your company is rolling out a training program to ensure that everyone is familiar with the company's IT usage policy. As a member of the Human Resources Department, you have been asked to develop a key piece of the training relating to why this policy is needed.

What kind of concerns can you expect your audience to raise? How can you deal with this anticipated resistance to the policy?

9. You work as part of the online marketing group for a midsized manufacturing company that has sales of more than $250 million per year and almost $50 million from online sales. You have been challenged by the vice president of sales to change the company's Web site data privacy policy from an opt-in policy to an opt-out policy and to allow the sale of customer data to other companies. The vice president has estimated that this change would bring in at least $5 million per year in added revenue with little additional expense. How would you respond to this request?

Cases

1. "Extraterritorial Jurisdiction" Puts Citizen Data at Risk

The legal doctrine of extraterritorial jurisdiction allows a government to claim the authority to extend its criminal laws beyond its geographical boundaries. For a claim of extraterritorial jurisdiction to be enforced, the legal authority in the external territory or a legal authority that covers both territories must approve its validity. For example, The Vienna Convention on Diplomatic Relations, an international treaty signed in 1961, specifies the legal privileges that enable diplomats to live and work in a foreign country without the threat of harassment by the host country; this treaty provides the legal basis for diplomatic immunity, which exempts diplomats (and their staff and families) from local judicial process and police interference.[77]

The concept of extraterritorial jurisdiction also has implications for personal data privacy. When personal data held by one organization is transferred to a third party for storage or processing, the original organization is still, by law, responsible for that data and must provide for its security while it is being held by the third party. This responsibility is typically met by including special provisions in the outsourcing contract that limits the third party's use or disclosure of the data. However, based on the concept of extraterritorial jurisdiction, some legal experts now believe that U.S. law enforcement and intelligence agencies could circumvent other countries' data privacy laws to gain access to data on citizens of foreign countries if that data is being stored by a company (foreign or U.S.) that conducts "systematic business" in the United States.[78]

If information about a country's citizens is transferred for storage or processing to a U.S. or U.S.-controlled foreign company, the U.S.-linked company could be compelled (via an NSL or a FISA court order) to grant access to that data. And a controversial section of the USA PATRIOT Act prohibits an organization from disclosing that it has received or disclosed data as a result of a FISA order. This could allow U.S. law enforcement and intelligence agencies to completely circumvent other countries' data privacy laws to gain access to citizen data—with no knowledge on the part of the foreign organization storing or processing the data or the citizens whose data was revealed.[79] Furthermore, since non-U.S. residents are not safeguarded by the Fourth Amendment (or other U.S. data privacy laws such as Electronic Communications Privacy Act), U.S. law enforcement and intelligence agencies could be free to gather data about non-U.S. citizens located abroad.

The Netherlands is one country particularly concerned about this possibility as it has just implemented the Dutch Electronic Patient Database, which puts the medical records of all Dutch nationals into a single patient database accessible to doctors.[80] The company that developed this system will be storing the patients' data on a cloud computing system run by CSC, a U.S.-based firm with operations in the Netherlands. Originally, the privacy of this data was thought to be secure because of contracts that clearly assign jurisdiction over the data to Dutch authorities. The Netherlands has rigorous data protection laws that protect patients' sensitive data. However, some researchers at Amsterdam University have raised concerns that U.S. government agencies could circumvent the Netherlands' data protection laws and request access to medical information on every single person in the Netherlands.[81]

Importantly, other countries have implemented laws similar to the USA PATRIOT Act that include comparable provisions to access citizen data outside their respective jurisdictions. This all raises serious questions about the degree to which one the data of one country's citizens is protected from another country in our increasingly interconnected and borderless online world. Indeed, Microsoft's UK Managing Director Gordon Frazer publicly admitted that neither his firm, nor any other firm, could guarantee that data about EU citizens stored in an EU-based data center would not leave the EU under any circumstances.[82]

Discussion Questions

1. As a result of the risk and uncertainty raised by the doctrine of extraterritorial jurisdiction, some industry experts believe that the use of multinational cloud computing service companies poses an increase in exposure of private, confidential data. Develop a strategy or line of reasoning that such service providers could use to allay the fear of its existing or potential clients.
2. Do research to find the current status of the so called "gag provision" of the USA PATRIOT Act that prohibits an organization served with an NSL or FISA warrant from revealing that fact. Do you believe that this clause of the USA PATRIOT Act should be ruled unconstitutional? Why or why not?
3. Do research to find at least three other countries that implemented legislature similar to the USA PATRIOT Act following the 9/11 terrorist attacks. Do these laws also lessen the restrictions for gathering intelligence data about the country's citizens?

2. Facebook Troubles with User Privacy

On Christmas 2012, Randi Zuckerberg posted a photo of her family to her private Facebook page. Unfortunately, the privacy settings on Facebook can confuse even the company's top executives. Randi, the sister of Facebook founder Mark Zuckerberg and a former senior Facebook executive, soon found that her photo had leaked to the general public and had been tweeted to thousands of people. Randi tweeted Callie Schweitzer, Director of Marketing at VOX Media, who had first posted the photo to Twitter: "Not sure where you got this photo. I posted it to friends only on FB. You reposting it to Twitter is way uncool."[83]

This incident came only 11 days after Facebook had released new privacy controls meant to help Facebook users understand who is able to see the content they post. A new shortcuts toolbar allowed users to control "Who can see my stuff" without having to go to a new page. The new release also offered in-product education. Messages explained how content that users

hide in their timelines could still appear in their news feed and on other pages.[84] Evidently, these controls did not go far enough to protect Randi Zuckerberg's privacy.

In fact, since Facebook was launched, it has had ongoing issues with addressing the privacy concerns of its users. In late 2011, Facebook settled a suit filed by the Federal Trade Commission (FTC) that charged Facebook with deceiving its customers about privacy issues since 2009. (The FTC regulates companies that take credit card information from consumers.) Facebook claimed that it would not share personal information with advertisers, that third-party applications would only be given the information they needed to function properly, that no one could access photos or videos from deleted accounts, and—perhaps most relevant to Randi Zuckerberg's experience—that information posted to an individual's Friends List would remain private. The FTC found that the company had not delivered on any of these claims. As part of the settlement, Facebook agreed to stop these practices until they had a better disclaimer and opt-out procedure. Mark Zuckerberg also issued a statement saying that, over the course of the previous 18 months, Facebook had introduced 20 new tools to address these and other privacy-related concerns.[85]

However, by August 2012, the FTC had launched a new investigation into Facebook privacy practices. Facebook had partnered with Datalogix—a company that collects credit card purchasing information, such as where users are shopping and what they buy. Facebook users were included in Datalogix advertising research although they were not informed of this. Moreover, if Facebook users did, in fact, find out about the use of their private data, they could only opt out of the research by going to the Datalogix homepage.[86]

Facebook has also had privacy problems arise with its subsidiaries. In September 2012, Facebook acquired Instagram, a social media application that allows users to upload photos for long-term storage and sharing. Instagram boasted a user-base of 100 million users. On December 17, 2012, Instagram posted a privacy notice claiming the right to sell all photographs posted to its site without compensation to the user. The company further claimed that it could sell any other metadata associated with the photo, such as usernames, gender, addresses, mobile phone number, and email addresses—all information users were required to provide when setting up an account.[87] Instagram asked users who did not agree with the notice to remove their accounts within a few weeks. The new policy would go into effect for all users who accessed their accounts after January 19, 2013.[88]

The announcement garnered a great deal of public resentment. On December 18, 2012, Instagram cofounder Kevin Systrom clarified that, despite the notice, the company had no current plans to sell users' photos. He explained that the company would be redrafting the privacy notice. In the meantime, competitors like Flickr have picked up a larger market share as a result of Instagram's privacy misstep.[89]

Facebook is a powerful tool for communicating and reconnecting with friends and family. The service it provides is so valuable that users continue to flock to it. However, with every step forward, Facebook seems to take one or two steps backward in its protection of user privacy. Whether at the hands of the FTC or the competition, Facebook will no doubt continue to face repercussions for its decisions.

Although Randi Zuckerberg may have blamed Callie Schweitzer for poor online manners, it is likely that most of the billion Facebook users would prefer to rely on some mechanism beyond social media etiquette to protect their photographs and private information.

Discussion Questions

1. Do you think that Facebook or careless, uninformed users should be held responsible for privacy issues related to using Facebook? Explain.
2. What additional measures should Facebook take to protect user privacy? What additional actions are required on the part of Facebook users to maintain adequate privacy?
3. Describe a privacy issue so serious that it would cause you to stop using Facebook.

3. Google Collects Unprotected Wireless Network Information

Google's Street View maps allow users to zoom into a location on a map and view actual images of houses, shops, buildings, sidewalks, fields, parked cars, and anything else that can be photographed from the vantage point of a slow-moving vehicle. It's a remarkable tool for those trying to find an auto repair shop, a post office, or a friend's house for the first time. Google launched Street View in a few cities in the United States in May 2007. It gradually expanded to additional U.S. cities and then to other cities around the world. In August 2009, Google began collecting data for Street View in several German cities. Germany, however, has stricter privacy laws than other countries, and prohibits the photographing of private property and people unless they are engaged in a public event, such as a sports match. As a result, Google had to work closely with the country's Data Protection Agency in order to comply with German laws in the hopes of getting its Street View service for Germany online by the end of 2010.[90,91]

In April 2010, a startling admission by Google provoked public outrage in Germany and around the world. It resulted in government probes in numerous countries, as well as several class action lawsuits in the United States. In response to queries by Germany's Data Protection Agency, Google acknowledged that, in addition to taking snapshots, its cars were also sniffing out unprotected wireless network information. Google reported that it was only collecting service set identifier (SSID) data—such as the network name—and the media access control (MAC) address—the unique number given to wireless network devices. Google's geo-location services could use this data to more accurately pinpoint the location of a person utilizing a mobile device, such as a smartphone. The company insisted that it was not collecting or storing payload data (the actual data sent over the network).[92]

The German Federal Commissioner for the Data Protection Agency was horrified and requested that Google stop collecting data immediately.[93] Additionally, the German authorities asked to audit the data Google had collected. Google agreed to hand over its code to a third party, the security consulting firm Stroz Friedberg. Nine days later there came another admission: Google had in fact been collecting and storing payload data. But Google insisted that it had only collected fragmented data and made no use of this data.[94] A few days later, Germany announced that it was launching a criminal investigation. Other European nations quickly opened investigations of their own.[95]

By early June, six class action lawsuits claiming that Google had violated federal wiretapping laws had been filed in the United States.[96] In its defense, Google argued that collecting unencrypted payload data is not a violation of federal laws.[97] Google explained that in order to locate wireless hotspots, it used a passive scanning technique, which had picked up payload data by mistake. The company used open source Kismet wireless scanning software that was customized by a Google engineer in 2006.[98] Google insisted that the project's managers were unaware that the software had been programmed to collect payload data when they launched

the project. Finally, Google argued that the data it collected was fragmented—not only was the car moving, but it was changing channels five times per second.[99]

However, a civil lawsuit claimed that Google filed a patent for its wireless network scanning system in November 2008 that revealed that Google's system could more accurately locate a router's location—giving Google the ability to identify the street address of the router. The more data collected by the scanning system, the lawsuit contended, the higher the confidence level Google would have in its calculated location of the wireless hotspot.[100]

In the fall of 2010, the U.S. Federal Trade Commission (FTC) ended its investigation, deciding not to take action or impose fines. The FTC recognized that Google had taken steps to amend the situation by ceasing to collect the payload data and by hiring a new director of privacy.[101] But by that time, 30 states had opened investigations into the matter.[102] During the course of these and other investigations, Google turned over the data it had collected to external regulators. On October 22, the company announced that not all of the payload data it had collected was fragmentary. It had in fact collected entire email messages, URLs, and passwords.[103] In November, the U.S. Federal Communications Commission announced that it was looking into whether Google had violated the federal Communications Act.[104]

Some analysts believe that Google's behavior follows a trend in the Internet industry: Push the boundaries of privacy issues; apologize, and then push again once the scandal dies down.[105] If this is the case, Google will have to decide, as the possible fines and other penalties accrue, whether this strategy pays off.

Discussion Questions

1. Cite another example of information technology companies pushing the boundaries of privacy issues; apologizing, and then pushing again once the scandal dies down. As long as the controversy fades, is there anything unethical about such a strategy?
2. Google states that its intention in gathering unprotected wireless network information was simply to be able to provide more accurate location data for its Street View service. Can you think of any reason for Google to have gathered this data? Is there any potential service Google could consider offering with this additional data?
3. Enter the street address of your home or place of work to find what photos are available in Street View. Comment on the accuracy of Street View and the content of the photos you find. Does this sort of capability delight you or concern you? Why?

End Notes

1 James Bamford, "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)," *Wired*, March 15, 2012, www.wired.com/threatlevel/2012/03/ff_nsadatacenter.

2 National Security Agency, "Utah Data Center," http://nsa.gov1.info/utah-data-center/index.html (accessed December 15, 2012).

3 James Bamford, "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)," *Wired*, March 15, 2012, www.wired.com/threatlevel/2012/03/ff_nsadatacenter.

[4] National Security Agency, "Utah Data Center," http://nsa.gov1.info/utah-data-center/index.html (accessed December 15, 2012).

[5] Cisco Systems, "Forecast For The Consumer IP Traffic Worldwide from 2011 to 2016," www.statista.com/statistics/152566/forecast-for-the-data-volume-internet-traffic-worldwide.

[6] Jaikumar Vijayan, "Groups Say FISA Law Needs More Oversight – Now," *Computerworld*, December 14, 2012, www.computerworld.com/s/article/9234740/Groups_say_FISA_law_needs_more_oversight_now.

[7] Ryan Singel, "NSA Chief Denies, Denies, Denies Wired's Domestic Spying Story," *Wired*, March 20, 2012, www.wired.com/threatlevel/2012/03/nsa-denies-wired.

[8] James Bamford, "NSA Chief Denies Domestic Spying But Whistleblowers Say Otherwise," *Wired*, March 21, 2012, www.wired.com/threatlevel/2012/03/nsa-whistleblower.

[9] "Foreign Intelligence Surveillance Act (FISA)," *New York Times*, http://topics.nytimes.com/top/reference/timestopics/subjects/f/foreign_intelligence_surveillance_act_fisa/index.html (accessed September 13, 2012).

[10] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, www.nytimes.com/2005/12/16/politics/16program.html, December 16, 2005.

[11] Privacy Protection Study Commission, "Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission," July 12, 1977, http://aspe.hhs.gov/datacncl/1977privacy/toc.htm.

[12] 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).

[13] 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).

[14] "The Fair Credit Reporting Act," www.ftc.gov/os/statutes/031224fcra.pdf (accessed December 13, 2012).

[15] U.S. Government Printing Office, "Gramm-Leach-Bliley Act," www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf (accessed December 19, 2012).

[16] U.S. Government Printing Office, "Fair and Accurate Credit Transactions Act," www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf (accessed December 12, 2012).

[17] George V. Hulme, "Protecting Privacy," *InformationWeek*, April 16, 2001.

[18] Sabrina Rodak, "Staffing Agency Employee at Providence Holy Cross in California Allegedly Posts Patient's Record on Facebook," *Becker's Hospital Review*, January 4, 2012, www.beckershospitalreview.com/healthcare-information-technology/providence-holy-cross-employee-in-california-allegedly-posts-patients-record-on-facebook.html.

[19] U.S. Department of Health and Human Services, "About the Office of Civil Rights," www.hhs.gov/ocr/office/about/index.html (accessed December 20, 2012).

[20] Pamela Lewis Dolan, "$100,000 HIPAA Fine Designed to Send Message to Small Practices," amednews.com, May 2, 2012, www.ama-assn.org/amednews/2012/04/30/bisd0502.htm.

[21] Lindsay Hutton, "Kids and Internet Usage: The Surprising Facts," *Family Education*, http://life.familyeducation.com/internet-safety/computers/58015.html (accessed December 26, 2012).

[22] 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.

[23] Ashley Post, "Celebrity Fan Sites Fined for COPPA Violations," *Inside Counsel*, October 11, 2012, www.insidecounsel.com/2012/10/11/celebrity-fan-sites-fined-for-coppa-violations.

[24] U.S. Department of Justice, "Federal Statutes Important in the Information Sharing Environment (ISE)," www.it.ojp.gov/default.aspx?area=privacy&page=1286 (accessed January 2, 2013).

[25] Electronic Privacy Information Center, "National Security Letters,", http://epic.org/privacy/nsl (accessed December 22, 2012).

[26] Ms. Smith, "Counterintelligence Surveillance Swelled Another 10% in 2011," *Network World*, May 9, 2012, www.networkworld.com/community/blog/counterint/elligence-surveillance-swelled-another-10-2011.

[27] U.S. Department of Justice, "Privacy & Civil Liberties: Title III of the Omnibus of the Crime and Safe Streets Act of 1968 (Wiretap Act)," www.it.ojp.gov/default.aspx?area=privacy&page=1284 (accessed February 11, 2013).

[28] *Katz v. United States*, 389 U.S. 247 (1967), http://supreme.justia.com/cases/federal/us/389/347/case.html (accessed February 11, 2013).

[29] Administrative Office of the U.S. Courts, "2011 Report Shows Decrease in Requests for Authorized Intercepts," June 29, 2012, http://news.uscourts.gov/2011-wiretap-report-shows-decrease-requests-authorized-intercepts.

[30] 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.

[31] "Communications Assistance for Law Enforcement Act (CALEA)," http://transition.fcc.gov/calea (accessed December 28, 2012).

[32] Electronic Privacy Information Center, "National Security Letters," http://epic.org/privacy/nsl (accessed December 22, 2012).

[33] "America Revealed: National Security Letters and Gag Orders," January 22, 2011, www.spaulforrest.com/2011/01/national-security-letters-and-gag.html.

[34] Eric Lichtblau and James Risen, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005.

[35] Eric Lichtblau and James Risen, "Officials Say U.S. Wiretaps Exceeded Law," *New York Times*, April 16, 2009.

[36] Eric Lichtblau and James Risen, "Officials Say U.S. Wiretaps Exceeded Law," *New York Times*, April 16, 2009.

[37] The Organisation for Economic Co-Operation and Development, "About the OECD," www.oecd.org/about (accessed December 29, 2012).

[38] The Organisation for Economic Co-Operation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (accessed December 28, 2012).

[39] Hunton & Williams LLP, "European Commission Finds New Zealand's Data Protection Law Provides Adequate Safeguards," December 20, 2012, www.huntonprivacyblog.com/tag/eu-data-protection-directive.

[40] Rebecca Herold, "European Union (EU) Data Protection Directive of 1995: Frequently Asked Questions," May 2002, www.informationshield.com/papers/EU%20Data%20Protection%20Directive%20FAQ.pdf.

[41] Export.gov, "Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks," www.export.gov/safeharbor (accessed February 6, 2011).

[42] "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase User's Control of Their Data and To Cut Costs for Businesses," European Commission – Press Release, January 25, 2012, http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

[43] "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase User's Control of Their Data and To Cut Costs for Businesses," European Commission – Press Release, January 25, 2012, http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

[44] Federal Communications Commission, "FOIA," www.fcc.gov/foia (accessed January 1, 2013).

[45] U.S. Department of Justice, "What is FOIA?" www.foia.gov (accessed January 1, 2013).

[46] Dale Eisinger, "Former Criminals Agree a Map of Gun Owners Is, er, Was a Good Thing," *Newsmax*, January 4, 2013, www.newsmax.com/TheWire/criminals-map-gun-owner/2013/01/04/id/470127.

[47] Leigh Goessl, "Controversy Over Published Map of NY Gun Permit Holders Escalates," *Digital Journal*, December 29, 2012, www.digitaljournal.com/print/articale/340080.

[48] Electronic Privacy Information Center, "The Privacy Act of 1974," http://epic.org/privacy/1974act (accessed January 1, 2013).

[49] Electronic Privacy Information Center, "Federal Appeals Court Affirms Civil Penalties in Privacy Act Case," https://epic.org/privacy/chao (accessed January 1, 2013).

[50] Greg Sandoval, "Veterans' Data Swiped in Theft," *CNET*, May 22, 2006, http://news.cnet.com/Veterans-data-swiped-in-theft/2100-1029_3-6075212.html.

[51] "Data Statistics," DataLossdb, www.datalossdb.org/statistics (accessed January 4, 2013).

[52] Law Research, "American Recovery and Reinvestment of 2009: Title XIII Health Information Technology," www.justlawlinks.com/ACTS/arara/araraA_title-XIII.php#subD (accessed December 21, 2012).

[53] "HITRUST's Analysis of U.S. Breach Data Finds Little Progress and Concern for Unreported Breaches," *Yahoo Finance*, December 5, 2012.

[54] National Conference of State Legislatures, "2012 Security Breach Legislation," www.ncsl.org/issues-research/telecom/security-breach-legislation-2012.aspx, December 13, 2012.

[55] Jaikumar Vijayan, "Hospital Appeals $250,000 Fine for Late Breach Disclosure," *Computerworld*, September 10, 2010, www.computerworld.com/s/article/9184679/Hospital_appeals_250_000_fine_for_late_breach_disclosure.

[56] Ellen Messmer, "Zappos Data Breach Response a Good Idea or Just Panic Mode?," *Network World*, January 12, 2012, www.networkworld.com/news/2012/011712-zappos-data-breach-254971.html.

[57] Greg Lamm, "Lawsuits Pour In Against Amazon in Zappos Hacking Breach," *Puget Sound Business Journal*, March 7, 2012, www.bizjournals.com/seattle/news/2012/03/07/lawsuits-pour-in-against-amazon-in.html.

[58] 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.

[59] "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.

[60] Keith Wagstaff, "Grading How Well Companies Are Cooperating With 'Do Not Track'," *Time*, May 21, 2012.

[61] "Policy, Enforcement May Stop Employees From Wasting Time Online at Work," *newswise/Kansas State University*, January 31, 2013, www.inquisitr.com/511795/employees-waste-up-to-80-percent-of-time-cyberloafing-study.

[62] "The Top Ten Ways Workers Waste Time Online," *24/7 Wall St.*, September 30, 2010, http://247wallst.com/2010/09/30/the-top-ten-ways-workers-waste-time-online.

[63] Nicole Blake Johnson, "When Employee Monitoring Goes Too Far," *Federal Times*, August 5, 2012, www.federaltimes.com/article/20120805/PERSONNEL03/308050005/When-employee-monitoring-goes-too-far.

[64] Jaikumar Vijayan, "FDA Defends Monitoring of Whistleblower's Email," *Computerworld*, February 12, 2012.

[65] Alex White, "CCTV Surveillance Will Remain After Olympics," *Security Blog*, August 27, 2012, http://blog.jammer-store.com/2012/08/cctv-surveillance-will-remain-after-olympics.

[66] Alastair Jamieson and Michele Neubert, "Fortress London: UK Protects Olympics with Biggest Security Plan Since World War II," *World News*, July 25, 2012, http://worldnews.nbcnews.com/_news/2012/07/25/12929477-fortress-london-uk-protects-olympics-with-biggest-security-plan-since-world-war-ii?lite.

[67] "Dramatic Expansion of DC Surveillance Camera Network," *Homeland Security Newswire*, February 1, 2011, http://homelandsecuritynewswire.com/dramatic-expansion-dc-surveillance-camera-network.

[68] "CTA Touts Success of Surveillance Cameras in Fighting Crime," *CBS Local*, October 26, 2012, http://chicago.cbslocal.com/2012/10/26/cta-touts-success-of-surveillance-cameras-in-fighting-crime/.

[69] "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.

[70] "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.

[71] 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.

[72] Collision Data Service, "EDR Legal Updates," http://edraccess.com/CaseLaw.aspx (accessed January 5, 2013).

[73] *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 January 7, 2013).

[74] "High-Tech Devices Leave Users Vulnerable to Spies," *Phys.Org*, January 5, 2012, http://phys.org/print244989742.html.

[75] "Are You Looking for the Best Spy Phone Software That Really Work?" www.spyphonesreview.com (accessed December 27, 2012).

[76] "Senate Takes Step Toward Banning Stalking Software," *PhysOrg.com*, December 13, 2012, phys.org/print274621361.html.

[77] Encyclopedia Britannica, "Extraterritoriality," www.britannica.com/EBchecked/topic/199129/extraterritoriality (accessed February 18, 2013).

[78] Zack Whittaker, "Patriot Act Can 'Obtain' Data in Europe, Researchers Say," *CNET*, December 6, 2012, http://news.cnet.com/8301-13578_3-57557569-38/patriot-act-can-obtain-data-in-europe-researchers-say.

[79] Zack Whittaker, "Patriot Act Can 'Obtain' Data in Europe, Researchers Say," *CNET*, December 6, 2012, http://news.cnet.com/8301-13578_3-57557569-38/patriot-act-can-obtain-data-in-europe-researchers-say.

[80] Richard Levy, "Privacy Row Over Putting Dutch Medical Charts on File," *Monsters & Critics*, November 12, 2008, mhttp://news.monstersandcritics.com/health/features/article_1442619.php/Privacy_row_over_putting_Dutch_medical_charts_on_file_News_Feature.

[81] Ben Zevenbergen, "US Government Agencies Will Soon Be Able to Access Foreign Medical Dossiers Due to Patriot Act, *Tech Dirt*, December 7, 2012, www.techdirt.com/articles/20121201/12234021198/us-government-agencies-will-soon-be-able-to-access-foreign-medical-dossiers-due-to-patriot-act.shtml.

[82] Zack Whittaker, "Patriot Act Can 'Obtain' Data in Europe, Researchers Say," *CNET*, December 6, 2012, http://news.cnet.com/8301-13578_3-57557569-38/patriot-act-can-obtain-data-in-europe-researchers-say.

[83] Terri Schwartz, "Randi Zuckerberg's Family Photo Leaks Because of Confusing Facebook Settings," *Zap2it*, December 27, 2012, http://blog.zap2it.com/pop2it/2012/12/randi-zuckerbergs-family-photo-leaks-because-of-confusing-facebook-settings.html.

[84] Debra Donston-Miller, "Facebook's New Privacy Policies: The Good News," *InformationWeek*, December 14, 2012, www.informationweek.com/thebrainyard/news/social_networking_consumer/240144443/facebooks-new-privacy-policies-the-good-news.

[85] Thomas Claburn, "Facebook Settles FTC Charges, Admits Mistakes," *InformationWeek*, November 29, 2011, www.informationweek.com/security/privacy/facebook-settles-ftc-charges-admits-mist/232200385.

[86] Jeff Goldman, "Privacy Concerns Raised Over Facebook-Datalogix Partnership," *eSecurity Planet*, September 25, 2012, www.esecurityplanet.com/network-security/privacy-concerns-raised-over-facebook-datalogix-partnership.html.

[87] Charles Arthur, "Facebook Forces Instagram Users to Allow It To Sell Their Uploaded Photos," *The Guardian*, December 18, 2012, www.guardian.co.uk/technology/2012/dec/18/facebook-instagram-sell-uploaded-photos.

[88] "Humbled Instagram Backs Down on Controversial Changes to Serve User Photos As Ads," *Independent.ie*, December 21, 2012, www.independent.ie/business/technology/humbled-instagram-backs-down-on-controversial-changes-to-serve-user-photos-as-ads-3333391.html.

[89] "Humbled Instagram Backs Down on Controversial Changes to Serve User Photos As Ads," *Independent.ie*, December 21, 2012, www.independent.ie/business/technology/humbled-instagram-backs-down-on-controversial-changes-to-serve-user-photos-as-ads-3333391.html.

[90] Jeremy Kirk, "Germany Launches Criminal Investigation of Google," *PCWorld*, May 20, 2010, www.pcworld.com/article/196765/germany_launches_criminal_investigation_of_google.html.

[91] Andrew Orlowski, "Google Street View Logs WiFi Networks, Mac Addresses," *The Register*, April 22, 2010, www.theregister.co.uk/2010/04/22/google_streetview_logs_wlans.

[92] Google "Data Collected by Google Cars," *European Public Policy Blog*, April 27, 2010, http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html.

[93] Andrew Orlowski, "Google Street View Logs WiFi Networks, Mac Addresses," *The Register*, April 22, 2010, www.theregister.co.uk/2010/04/22/google_streetview_logs_wlans/.

[94] Google, "WiFi Data Collection: An Update," *The Official Google Blog*, May 14, 2010, http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.

[95] Kevin O'Brien, "In Europe, Google Faces New Inquiries on Privacy," *New York Times*, May 20, 2010.

[96] Robert McMillan, "Google WiFi Uproar: Six Class Action Lawsuits Filed," *TechWorld*, June 4, 2010, http://news.techworld.com/networking/3225722/google-wifi-uproar-six-class-action-lawsuits-filed.

[97] David Kravets, "Packet-Sniffing Laws Murky as Open Wi-Fi Proliferates," *Wired*, June 22, 2010.

[98] Tom Krazit, "Deciphering Google's Wi-Fi Headache (FAQ)," *CNET*, June 1, 2010, http://news.cnet.com/8301-30684_3-20006342-265.html.

[99] Google, "WiFi Data Collection: An Update," *The Official Google Blog*, May 14, 2010, http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.

[100] Gregg Keizer, "Google Wants to Patent Technology used to 'Snoop' Wi-Fi Networks," *Computerworld*, June 3, 2010, www.computerworld.com/s/article/9177634/Google_wants_to_patent_technology_used_to_snoop_Wi_Fi_networks.

[101] Matt McGee, "FTC Ends Google WiFi Inquiry, No Penalties Announced," *Search Engine Land* (blog), October 27, 2010, http://searchengineland.com/ftc-ends-google-wifi-inquiry-no-penalties-54058.

[102] Tom Krazit, "Connecticut Heads Up 30-State Google Wi-Fi Probe," *CNET*, June 21, 2010, http://news.cnet.com/8301-30684_3-20008332-265.html.

[103] Alan Eustace, "Creating Stronger Privacy Controls Inside Google," *Google Public Policy Blog*, October 22, 2010, http://googlepublicpolicy.blogspot.com/2010/10/creating-stronger-privacy-controls.html.

[104] Chloe Albanesius, "FCC Investigating Google Street View Wi-Fi Data Collection," *PCMag.com*, November 10, 2010, www.pcmag.com/article2/0,2817,2372498,00.asp.

[105] Tom Krazit, "Deciphering Google's Wi-Fi Headache (FAQ)," *CNET*, June 1, 2010, http://news.cnet.com/8301-30684_3-20006342-265.html.

CHAPTER 5

FREEDOM OF EXPRESSION

QUOTE

It is easy to believe in freedom of speech for those with whom we agree.
—Leo McKern, Australian actor

VIGNETTE

Reputation Changer, Online Reputation Management Company

Many consumers now use the Internet to research businesses and products and to make price comparisons prior to making a variety of purchases. In addition to the information that can be found on company Web sites, reviews of a variety of products and services are available on many online forums. Because of this, even solid companies that offer excellent products and services are increasingly concerned about the potential for gaining a negative online reputation due to comments made by a small number of disgruntled consumers—or even former employees or competing businesses. Misleading, inaccurate, or negative posts can have a damaging, long-term impact on a business.

In the past several years, a new type of company has emerged to help businesses manage potentially damaging information on the Web. Online reputation management companies offer a range of services to organizations including:

- Scanning the Internet to find references to a company (or its products or services) on social networks, blogs, and other Web sites

- Summarizing this data to show how a company is perceived by the general public
- Identifying specific negative posts that are hurting a business
- Helping a business create positive content that will suppress negative posts
- Managing search engine results to ensure that a company appears on the first page of search results
- Suppressing defamatory posts, including negative Better Business Bureau ratings

An online reputation management company can help a company be proactive in identifying negative posts and taking action to counteract these posts. Often, these firms will create original, positive posts for a business or product that can repair the damage done by negative posts. By posting new positive content, negative posts and reviews are pushed further down in search results. With enough new, positive content, the negative comments can be pushed entirely off the first page of search results.

One such reputation management company, Reputation Changer, was founded in 2009 and has over 100 employees with annual revenues above $10 million. The company boasts that it has thousands of satisfied clients from individual professionals, politicians, celebrities, and politicians to Fortune 500 companies.[1] One client testimonial posted on Reputation Changer's Web site relates how the client's online reputation was cast in a negative light due to an unfavorable news story about the firm. This story populated the first few pages of a Google search on the firm's name. Reputation Changer and the firm released a large number of positive press releases, company and product reviews, and blog entries that quickly moved to the front of the Google searches. As a result, the online reputation damage to the firm was minimized, with people's attention shifted to the more positive stories about the firm rather than the one negative news release.[2]

Questions to Consider

1. Do you think the use of an online reputation management company to suppress negative comments and boost positive comments is ethical?
2. Could the suppression of negative comments be considered an act in violation of the freedom of expression?

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 expression are not protected under the law?
2. What are some of the 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 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.

FIGURE 5-1 The U.S. Constitution
Credit: Image copyright Kasia, 2009. Used under license from Shutterstock.com.

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 and freedom of expression. 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. 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 if they believe someone has made a libelous attack against them. As an example, Beef Products, Inc. decided to sue ABC News, Inc. for $1.2 billion in a defamation lawsuit to protect the reputation of one of the company's meat products known as lean, finely texture beef. BPI alleges that ABC misled consumers into believing that consumption of the product was unsafe when the news organization referred to the product as "pink slime."[3] ABC has asked the court to throw out the case because it threatens free speech and inhibits the right of a news organization to report on matters of "obvious public interest."[4] ABC is employing two strong counterarguments that are frequently used in defamation cases, which are difficult to win.

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 freedom of expression, including controlling access to information on the Internet, anonymity on the Internet, defamation and hate speech, and pornography.

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 and violating First Amendment rights. 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 (CDA)

The **Telecommunications Act** became law in 1996. Its primary purpose was to allow freer 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.[5] 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."[6] 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 Web sites would probably either not exist or would look much different today had the law not been overturned. Web sites that might have been deemed indecent under the CDA would be operating under an extreme risk of liability.

Section 230 of the CDA 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.[7] This portion of the CDA was not ruled unconstitutional, and it is the reason why social networking companies such as Facebook, Twitter, and others cannot be sued for defamation for user postings that appear on their sites.

A blogger was sued for defamation when someone posted comments on his site stating that a professional football cheerleader was promiscuous and had contracted two sexually transmitted diseases. As part of his defense, the blogger claimed that his site was similar to Facebook or Twitter in that it simply served as a forum featuring user content. However, the blogger posted a response to one of the postings, thus moving himself into a gray area between content publisher and content provider.[8]

Child Online Protection Act (COPA)

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], discussed in Chapter 4. COPPA is directed at Web sites 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." (Subsequent sections of the act allow for penalties of up to $150,000 for each day of violation.)[9]

The law 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—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.[10] 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 Web sites 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 Web sites. With dynamic content filtering, each Web site'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. Studies by various organizations (Kaiser Family Foundation, Consumer Reports, the Free Expression Policy Project, and the San Jose Public Library) found that filters block Web sites containing useful information about civil rights, health, sex, and politics as well as online databases and online book catalogs.[11]

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 Web sites.

According to TopTenREVIEWS, the top rated Internet filters for home users for 2013 include Net Nanny Parental Controls, McAfee Safe Eyes, and McAfee Family Protection.[12] Safe Eyes® from InternetSafety.com™ is Internet filtering software that filters videos on YouTube, manages the viewing of online TV by choosing the 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. Internet software filters have also been developed to run on mobile devices such as Android, iPhone, and Microsoft smartphones. See Figure 5-2.

FIGURE 5-2 Screenshot of Safe Eyes® from Internet Safety
Source Line: Used with permission from InternetSafety.com, part of McAfee Inc.

Another approach to restricting access to Web sites 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 ISP, ClearSail/Family.NET, prevents access to known Web sites 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.[13]

Children's Internet Protection Act (CIPA)

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 Web sites 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.[14]

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, 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 Web sites 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. At least one federal court has ruled that a local library board may not require the use of filtering software on all library computers connected to the Internet. 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.

The ACLU filed a suit to challenge CIPA, and in May 2002, a three-judge panel in eastern Pennsylvania held that "we are constrained to conclude that the library plaintiffs must prevail in their contention that CIPA requires them to violate the First Amendment rights of their patrons, and accordingly is facially invalid" under the First Amendment. The ruling instructed the government not to enforce the act. This ruling, however, was reversed in June 2003 by the U.S. Supreme Court in *United States v. American Library Association.* The Supreme Court, in a 6-3 decision, held that public libraries must purchase filtering software and comply with all portions of CIPA.[15]

Internet Censorship

Internet censorship is the control or suppression of the publishing or accessing of information on the Internet. Censorship can take many forms—such as limiting access to certain Web sites, allowing access to only some content or modified content at certain Web sites, rejecting the use of certain keywords in search engine searches, tracking and monitoring the Internet activities of individuals, and harassing or even jailing individuals for their Internet use.

China has the largest online population in the world, with over 538 million Internet users (see Table 5-1, which depicts the top five countries in terms of number of Internet users). However, Internet censorship in China is perhaps the most rigorous in the world. Table 5-2 provides examples of Internet censorship in several countries.

TABLE 5-1 The top five countries with the highest number of Internet users June 30, 2012

Country	Population (million)	Internet users (million)	% of country's population
China	1,343	538	40.1%
United States	313	245	78.1%
India	1,205	137	11.4%
Japan	127	101	79.5%
Brazil	194	88	45.6%

Source Line: "Top 20 Countries with the Highest Number of Internet Users," Internet World Stats, © June 30, 2012, www.internetworldstats.com/top20.htm.

TABLE 5-2 Internet censorship examples by selected country

Country	Form of censorship
Brazil[16]	Brazilian government demands have closed more Google Gmail accounts and more blogger 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.
Myanmar[17]	Dissemination of information via the Internet is tightly monitored and controlled. Two high-ranking government officials were sentenced to death for emailing documents abroad.
China[18]	The government blocks access to Web sites 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 Web sites also employ censors who monitor and delete objectionable content. The government hires workers to post comments favorable to the government.
Cuba[19]	The ability to go on the Internet requires special permission so that only 2% of its population is online, and when a user does get connected, it is only to a highly censored version of the Internet.
Egypt[20]	Although Egypt had not set up an Internet filtering system under the regime of Hosni Mubarak, it did track Internet posters and arrest bloggers who made posts that were unacceptable to the Mubarak government. The government also disabled access to the Internet completely for periods of time.
United States[21]	Many in the United States feel that U.S. laws relating to the interception of online communications do not provide sufficient privacy guarantees for users. There are also concerns that some U.S. companies are selling equipment and technology to the Chinese government that enable it to censor Internet content for users in China.

Source Line: Copyright © Cengage Learning. Adapted from multiple sources. See End Notes 16, 17, 18, 19, 20, and 21.

Strategic Lawsuit Against Public Participation (SLAPP)

A **strategic lawsuit against public participation (SLAPP)** is a strategy employed by corporations, government officials, and others against citizens and community groups who oppose them on matters of public interest. A SLAPP is typically without merit and is used to intimidate critics out of fear of the cost and effort associated with a major legal battle. Many would question the ethics and legality of using a SLAPP; others would 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.[22]

Every year thousands of people become SLAPP victims due to their participation 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, or circulating a petition.[23] For example, a New Jersey man recently spoke out against a proposal to build an apartment complex in his neighborhood and soon after found himself the defendant in a $2.5 million defamation lawsuit. The plaintiff, the developer of the complex, claimed that he had suffered "disgrace, humiliation and shame throughout the community, permanent harm to his professional and personal reputations, and severe mental anguish and emotional distress."[24]

Anti-SLAPP laws are designed to reduce frivolous SLAPPs. Twenty-six states and the District of Columbia have put into effect anti-SLAPP legislature to protect people who are victims of a SLAPP.[25] While these laws vary from state to state, most are designed to quickly identify if there are any merits to the lawsuit and to keep lawyer fees to a minimum. There is no federal anti-SLAPP law as of yet.[26]

As an example of the effective use of anti-SLAPP legislation, consider the case of a California man who discovered that his business partner had opened a credit card in the name of the business at a local bank. The businessman went to the bank, closed the account, and informed bank employees that his partner had committed fraud. The partner sued the businessman for defamation, but the man's attorney was able to protect him by employing the state's anti-SLAPP legislation.[27]

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 from 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 when the population of the colonies was estimated to have been less than 4 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 Internet service provider 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.[28]

Doxing involves the examination of Internet records in an attempt to reveal the identity of an anonymous poster. For example, a doxer looking to track down the identity of someone who posted in a discussion forum on one Web site might search for clues to the poster's identity on Facebook, Twitter, and other online sources. Some view such activity as the equivalent of a helpful Neighborhood Watch. Others liken the activity to an online vigilante group with the potential of causing harm by identifying incorrect parties.[29]

Amanda Todd was a bullied Canadian teenager who committed suicide after posting a video on YouTube chronicling years of bullying online and in school.[30] The hacktivist group Anonymous then published the name and address of a man that the group claimed was responsible for bullying Todd online. That man was then threatened online by others vowing to carry out vigilante justice.[31]

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 would like to ban Web anonymity because they think its use increases the risks of defamation, fraud, libel, and the exploitation of children.

When an email is sent, the email software (e.g., 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 a relay server. 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 bogus one. This ensures that no header

information can identify the author. Some remailers route messages through multiple remailers to provide a virtually untraceable level of anonymity.

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.

In the spring of 2012, an email server in New York City operated by the European Counter Network (ECN), an ISP headquartered in Europe, was seized based on a search warrant issued at the request of the FBI.[32] The server was allegedly used to provide an anonymous remailer service that delivered over 100 bomb threat messages against the University of Pittsburgh to various local news outlets. The threats emptied classrooms and disrupted classes.[33]

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 Web site 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 Verizon, NetZero/Juno, and Earth Link—and social media 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 on the Internet 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*[34] 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 Pre-Paid message board. Attorneys for PPLS argued that it 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 Electronic Frontier Foundation (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 the *Doe v. 2TheMart.com, Inc*.[35] case 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 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.

In August 2001, a judge in Santa Clara County Superior Court invalidated the subpoena to Yahoo! 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 Web site 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 do not have the resources to prescreen content (and they do not assume any responsibility for content provided by others), many ISPs 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, how egregious the content is, and the general availability of ISP 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.[36] 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.[37]

Because such prohibitions are included in the service contracts between a private ISP and its subscribers, and do not involve the federal government, they do not violate the subscribers' First Amendment rights. Of course, ISP subscribers who lose an account for violating the ISP's regulations may resume their hate speech by simply opening a new account with some other, more permissive ISP.

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 considered 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 he subjects himself to the jurisdiction of that country—for example, by visiting there. As long as the person remains in the United States, he 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

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 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 a huge array of pornography Web sites—some estimates are as high as 24 million pornography sites worldwide.[38] 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 (however, revenue estimates vary widely between $1 billion and $97 billion)[39] and generates a lot of traffic; it is estimated that there are over 72 million visitors to pornographic Web sites monthly.[40]

Pornography purveyors are free to produce and publish whatever they want; however, if what they distribute or exhibit 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 Child Online Protection Act (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.[41] 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."[42] 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. A Nielsen survey on the viewing of pornography in the workplace revealed that 21 million Americans accessed porn from their work computers in March 2010—29 percent of the workforce.[43] 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.

There are numerous federal laws addressing issues relating 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. According to a survey by the National Campaign to Prevent Teen and Unplanned Pregnancy, one in five teenagers has sent or posted nude or seminude photos of himself/herself, including 22 percent of teen girls, 18 percent of teen boys, and 11 percent of young teen girls aged 13 to 16.[44] Now there is even a smartphone app, Snapchat, that enables users to send messages and share videos or images that disappear after a few seconds. However, users should be aware that recipients can take screenshots of a Snapchat on their phone, and an apparent security flaw enables recipients to retrieve deleted videos sent via Snapchat.[45]

Increasingly, sexters 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.

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

The **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act** (2003) 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 Web sites, 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 4 million posts. Of course, the spammer was unable to pay the fine and instead declared bankruptcy.[46]

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 United Kingdom recently fined two people £440,000 (about $700,000 USD) for sending out as many as 800,000 spam text messages per day to cell phone users on behalf of claims management companies looking for accident victims to pass on to lawyers.[47]

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 Web sites. 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.[48]

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.

Table 5-3 is a manager's checklist for dealing with issues of freedom of expression in the workplace. In each case, the preferred answer is *yes*.

TABLE 5-3 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 Web sites (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 IT usage 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?		

Source Line: Course Technology/Cengage Learning.

Summary

- The Internet enables a worldwide exchange of news, ideas, opinions, rumors, and information. Its broad accessibility, open discussions, and anonymity make it a powerful communications medium. People must often make ethical decisions about how to use such remarkable freedom and power.
- Organizations and governments have attempted to establish policies and laws to help guide Internet use as well as 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 First Amendment protects Americans' rights to freedom of religion and freedom of expression. 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.
- 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 and violating First Amendment rights.
- 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 unconstitutional. However, Section 230 of the Communications Decency Act was not ruled unconstitutional and provides immunity 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.
- 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 on Internet censorship.
- A SLAPP (strategic lawsuit against public participation) is a strategy of filing a lawsuit against citizens and community groups who oppose them on matters of concern.
- Anti-SLAPP laws are designed to reduce frivolous SLAPPs. Twenty-six states and the District of Columbia have put into effect anti-SLAPP legislature to protect people who are victims of a SLAPP.

- 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 the examination of Internet records in an attempt to reveal the identity of an anonymous poster.
- 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 have caused some form of harm 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 have voluntarily agreed to prohibit their subscribers from sending hate messages using their services. Because such prohibitions can be included in the service contracts between a private ISP and its subscribers, and do not involve the federal government, they do not violate subscribers' First Amendment rights.
- Many adults and 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.
- The key question in deciding what Internet material is obscene is: "Whose community standards are used?"
- Sexting—sending sexual messages, nude or seminude photos, or sexually explicit videos over a cell phone—is a fast-growing trend and can lead to many problems for both senders and receivers.
- The CAN-SPAM Act specifies requirements that commercial emailers must follow in sending out messages that advertise a commercial product or service. The CAN-SPAM Act can also be used in the fight against the dissemination of pornography.

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
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)
Telecommunications Act

Self-Assessment Questions

The answers to the Self-Assessment Questions can be found in Appendix B.

1. The _____ to the U.S. Constitution was adopted to guarantee the right to freedom of expression.
2. An important Supreme Court case that established a three-part test to determine if material is obscene and therefore not protected speech was _____.
3. The right to freedom of expression is restricted when the expressions, whether spoken or written, are untrue and cause harm. True or False?
4. Because defamation is defined as an untrue statement of fact, truth is an absolute defense against a charge of defamation. True or False?
5. _____ of the Communications Decency Act 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. Child Online Protection Act
   c. Children's Internet Protection Act
   d. Communications Decency Act
7. _____ is the control or suppression of the publishing or accessing of information on the Internet.
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 the examination of Internet records in an attempt to reveal the identity of an anonymous poster.
10. All anonymous email and blog postings are either illegal or unethical. True or False?

11. A(n) _____ lawsuit can be filed against a defendant whose identity is temporarily unknown because he or she is communicating anonymously or using a pseudonym.
12. 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 or not to approve subpoenas requesting the identity of anonymous Web posters
    d. whether speech is merely annoying or hate speech
13. A person who posts material on the Web that is illegal in a foreign country can be prosecuted if he visits that country; however, U.S. laws do not allow a person to be extradited for an activity protected by the U.S. Constitution. True or False?
14. Pornography purveyors are free to produce and publish whatever they want; however, if what they distribute or exhibit is judged obscene, they are subject to prosecution under obscenity laws. True or False?
15. Sexting is a fast-growing trend among U.S. teenagers. True or False?
16. The _____ Act specifies requirements that commercial emailers must follow in sending out messages that advertise or promote a commercial product or service.

Discussion Questions

1. Two frequently heard phrases associated with the 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. Briefly discuss attempts to create laws protecting children from harmful material on the Internet. Why were early attempts found to be unconstitutional?
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. 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.
5. Can you cite a specific example of federal government Internet censorship in the United States? Do you think the amount of Internet censorship in the United States is appropriate or overly restrictive? Explain your answer.
6. Do research to identify the current countries that are identified as "Enemies of the Internet" by the group Reporters Without Borders. What criteria did Reporters Without Borders use when deciding which countries to place on this list?
7. What can an ISP do to limit the distribution of hate email? Why would such actions not be considered a violation of the subscriber's First Amendment rights?

8. 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 or a loved one?
9. Why must U.S. organizations be very careful when dealing with issues relating to pornography in the workplace? What are some legal and reasonable steps an organization can take to limit pornography in the workplace?
10. Do research on the Web 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?
11. 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 email in the future?
12. 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?
13. Do you think further efforts to limit the dissemination of pornography on the Internet are appropriate? Why or why not?
14. How did the Children's Internet Protection Act 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.
15. Attempt to perform doxing to link some of your online postings to another posting that in turn links back to a posting that reveals your identity. Write a paragraph documenting your research and ultimate success or failure.

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 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 letters to the local newspaper voicing their displeasure with your candidate's actions in his initial term as mayor. The campaign manager has suggested that you file at least three defamation 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. How would you respond to this suggestion?
2. A former high school classmate of yours who moved to China emails you that he has been offered a part-time job monitoring a Chinese Web site and posting comments favorable to the government. How would you respond?

3. Your 15-year-old nephew exclaims “Oh wow!” and proceeds to tell you about a very revealing photo attachment he just received in a text message from his 14-year-old girlfriend of three weeks. He can’t wait to forward the image to others in his school using the Snapchat application on his phone. What would you say to your nephew? Are further steps needed besides a discussion on sexting?
4. 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 sexual discrimination observed during his five years as an employee with the firm. What would you say to your friend?
5. 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 negative posters with a libel lawsuit unless they remove their posting. Should that fail, the firm would generate dozens of positive postings to outweigh the negative posting. What would you say to your friend about her idea?
6. You are the computer technical resource for a county’s public library system. The library is making plans to install Internet filtering software so it will conform to the Children’s Internet Protection Act and be eligible for federal funding. What sort of objections can you expect regarding implementation of Internet filters? How might you deal with such objections?
7. 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?
8. 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 downloads from adult porn sites on the hard drive. What would you do?
9. A friend contacts you about joining his company, Anonymous Remailers Anonymous. He 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 increase 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, he admits it is possible that hackers and terrorists may use his firm’s services. Would you accept the generous job offer? Why or why not?
10. You are a member of the Human Resources Department and are working with a committee to complete your company’s computer usage policy. What advice would you offer the committee regarding how to address online pornography? Would you suggest that the policy be laissez-faire, or would you recommend that the committee require strict enforcement of tough corporate guidelines? Why?

Cases

1. Lawsuits Aimed at Yelp and Its Reviewers

Yelp is an online local directory service that combines customer reviews and social networking features. A visitor to the Yelp site can search for a particular type of service (e.g., dog grooming) within a specific geographic area (zip code, city, etc.). Yelp then provides business listings that meet the user's criteria along with a rating, reviews provided by users of the service, and other useful information such as business hours, address and phone number, and parking information. Yelp was founded in 2004 and earns revenue by selling ads to local businesses.[49]

Research by two Berkeley economists has shown that Yelp reviews can have a significant impact on the success of a business. For example, just a half-star increase on Yelp's 5-star rating scale makes it 30 to 49 percent more likely that a restaurant will sell out its 6-8 pm seating. The researchers concluded that online rating services "play an increasingly important role in how consumers judge the quality of goods and services."[50]

Yelp does not censor reviews and accepts reviews from friends as well as competitors of a business. As with other online rating services, Yelp has received criticism over the fairness of its reviews and has been accused of allowing fake reviews to be posted. However, Section 230 of the Communications Decency Act of 1996 protects Yelp from defamation lawsuits brought based on reviews that users post to its Web site.[51]

During 2010, several lawsuits emerged that claimed Yelp extorted businesses to advertise on the Web site in exchange for positive reviews. Yelp strongly denied the charges and eventually a judge granted the firm's request to dismiss the suits. However, the charges did cause Yelp to modify its review process. The firm discontinued its practice of allowing businesses that advertise with it to position their favorite review above all others. In addition, Yelp now allows users to see reviews that were deleted by its automated review process, which was designed to prevent business owners from posting too many positive reviews of their own business or strongly negative reviews of competitors.[52]

Online reviewers sometimes find themselves facing unpleasant consequences over what they have said in a review. An owner of a business may decide to confront a reviewer, either via online forums or emails, or in an actual face-to-face encounter. In addition, a 2012 Yelp reviewer was hit with a $750,000 defamation lawsuit and ordered to alter her derisive review of a home contractor, which included charges of jewelry theft.[53,54]

Discussion Questions

1. Visit Yelp's Web site (*www.yelp.com*) and search for reviews for a service from a local business with which you are familiar. Do you notice any reviews that are overly negative or that seem to border on defamation based on your experience with this business? Are there any reviews that are so positive that they sound like they were written by or paid for by the owner? Imagine that you are the Web site owner and want to automatically filter out such reviews. How might you do this in an ethical manner?
2. Brainstorm possible actions that a local business owner can take to offset the negative publicity associated with an especially bad review—identify both ethical and unethical actions.
3. What risks do you run in posting online reviews?

2. WikiLeaks Continues to Post Classified Materials

In September 2011, WikiLeaks (a nonprofit organization whose goal is to "bring important news and information to the public"[55]) published more than 250,000 secret U.S. diplomatic cables on its Web site.[56] Included in this cache of private communications between employees of the U.S. Department of State were requests made of U.S. diplomats serving in overseas embassies to gather intelligence information for the purpose of espionage. Specifically, diplomats were tasked with collecting personal information on foreign officials including email addresses, credit card numbers, and even frequent flier account numbers.[57]

These documents were made public less than a year after WikiLeaks' monumental release of approximately 400,000 top secret U.S. Army documents—a leak believed to be the largest in U.S. history.[58] The leaked Army documents purportedly uncovered instances in which American soldiers stood aside as the Iraqi Shiite-dominated security forces tortured Sunni prisoners. The documents also allegedly disclosed an additional unreported 15,000 civilian deaths during the Iraq War.[59] This "document dump" was in fact the third major leak of U.S. military secrets of 2010. In April, the organization had posted a video of U.S. Army helicopter carrying out an operation in which civilians and two Reuters reporters were killed in Iraq. Then in July, WikiLeaks posted 92,000 military memos that supposedly confirmed that Pakistan's intelligence agency regularly met with Taliban fighters.[60]

The United States government, meanwhile, tried feverishly to prosecute WikiLeaks and prevent future leaks. However, the First Amendment guarantees citizens freedom of the press and very few restrictions have been permitted by the U.S. Supreme Court. The most notable instance of that judicial restraint is when President Richard Nixon attempted to seek an injunction against the publication of the Pentagon Papers, containing military secrets from the Vietnam War, and the U.S. Supreme Court refused.[61] In 2010, the Congressional Research Service issued a report in which they concluded that no publisher of leaked information has ever been prosecuted for publishing the material, due to the implications for the First Amendment. As a result, the only legal action the U.S. government could take was to charge an Army soldier, Bradley Manning, with violating the Espionage Act for purportedly supplying WikiLeaks with the video of the helicopter and other classified documents. Prosecutors plan to present classified documents in court to show that the terrorist group Al Qaeda has benefited from the secret documents that Manning supplied WikiLeaks. Meanwhile, the judge has ruled that Manning, who was kept naked in a windowless room for as long as 23 hours a day, was subject to confinement "more rigorous than necessary" while he awaited his trial, which was scheduled to begin in the summer of 2013.[62]

Shortly after this third leak, several major Internet companies began to shut off services to WikiLeaks. These included PayPal and Moneybookers, two sites that WikiLeaks' supporters had used to contribute funds to the organization.[63] After massive denial-of-service attacks on WikiLeaks' site, the organization moved to Amazon servers.[64] Within a couple of days, however, Amazon decided it would no longer host the site.[65] The following day, December 3, 2010, the American domain name system provider EveryDNS.net took the domain offline. WikiLeaks supporters and volunteers responded immediately. Two days later, 208 WikiLeaks mirror sites were operating.[66] On December 7, Julian Assange, the editor-in-chief of WikiLeaks, was arrested in London at about the same time on rape charges issued from Sweden.[67] Assange fought extradition to Sweden and eventually sought and found asylum in the Ecuadoran embassy in

London. Even from asylum, Assange continues to vex the U.S. government, hosting a video conference at the United Nations on U.S. efforts to combat WikiLeaks.[68]

As this online and offline battle rages, the public and the media have expressed a range of views. Many argued that WikiLeaks has endangered national security. Others staunchly defended WikiLeaks and its freedom to publish leaks. WikiLeaks came under criticism from human rights organizations and the international free press group Reporters Without Borders. Thousands of documents contained the names of Afghan informants, whose identity was now exposed and so could be targeted by the Taliban in reprisal for their collaboration.

Assange's actions also provoked dissent within the WikiLeaks organization. Some WikiLeaks staff felt that Assange had ignored hundreds of leaks from other regions of the world, in order to target the U.S. government. About half-a-dozen staffers resigned in the months after Assange was charged with rape.[69] These staffers called attention to an important point. WikiLeaks' Facebook page claims "Our primary interest is in exposing oppressive regimes in Asia, the former Soviet bloc, Sub-Saharan Africa and the Middle East…." Yet the overwhelming majority of its documents released in 2010 targeted one of the largest and most stable democracies in the world, the United States.

Julian Assange, WikiLeaks' very public leader, states that his objective is to establish a new standard of scientific journalism. He has published WikiLeaks' analysis of source material along with the source material itself, so that the readers themselves can come to their own conclusions.[70] Yet like other media sources, he, his staff, and his volunteers choose which sources to share, and this choice is colored by their own ideology and purposes. What these are, however, is difficult to ascertain. While WikiLeaks advocates for transparency in government and corporations, uncovering their secrets, the organization itself is far from transparent, keeping the identity of most of its members and contributors secret. The organization relies on a few staffers and hundreds of volunteers from around the world. Key volunteers are known by their initials only, even within encrypted online chats.[71] Hence, the question of WikiLeaks' bias or motivation or ultimate purpose cannot be definitively resolved.

In the summer of 2012, WikiLeaks posted over two million emails documenting communication between Syrian government officials and private companies. WikiLeaks claims on its homepage that these documents showed that Western companies supported the Syrian government, which has killed thousands of civilians in a brutal civil war.[72] Clearly, WikiLeaks would like to portray itself as an advocate for civil liberties and human rights. However, it is as yet unclear what the political ramifications of its leaks will be, and whether the leaks will have a positive or negative impact on democratic governments around the world.

Discussion Questions

1. How does the First Amendment protect WikiLeaks from prosecution?
2. Is WikiLeaks justified in releasing Syrian government emails? Is this different from posting classified U.S. documents?
3. What limits, if any, should be placed on WikiLeaks' right to post government or corporate secrets?

3. Facebook, Freedom of Speech, Defamation, and Cyberbullying

In February 2009, Oceanside High School graduate Denise Finkel sued Facebook, four former classmates, and their parents for false and defamatory statements made against her.[73] The classmates, part of a private Facebook group called "90 Cents Short of a Dollar," had posted comments to a password-protected page alleging that Finkel used intravenous drugs, had AIDS, and had engaged in inappropriate sexual behavior.[74]

Many legal commentators found the case surprising. Why would an attorney sue Facebook, when the company is obviously protected by Section 230 of the Communications Decency Act (CDA)? The CDA protects Web site owners from liability for content posted by a third party. Thus, Facebook should be immune from defamation lawsuits that arise from user-posted content.[75] However, Finkel claimed that Facebook's Terms of Use agreement established Facebook's proprietary rights to the site's content. In support of this argument, she pointed to the following clause in the agreement: "All content on the site … [is] the proprietary property of the Company, its users or licensors with all rights reserved."[76] As a result of this unique argument, the case attracted national attention because the consequences of the ruling could have serious implications for other social media sites. In September 2009, however, the Supreme Court of New York ruled that the Terms of Use did not disqualify Facebook from immunity under the CDA.[77]

This ruling provoked commentary by legal professionals, but no one was very surprised. What was less predictable was whether or not the court would hold Finkel's classmates liable. To what extent do students have the right to exercise their freedom of speech through social media outlets? What restrictions have been placed on this freedom?

In July 2010, the New York Supreme Court dismissed the case against Finkel's former classmates. The court determined that teenage members of the "90 Cents Short of a Dollar" Facebook group had simply acted childishly and were not guilty of defamation.[78] Finkel did not have any recourse against her former classmates via an antibullying statute because although the state of New York has a law prohibiting bullying, it only prohibits bullying on school property. The law does not apply to cyberbullying. Furthermore, the law merely requires that the schools take disciplinary action, and it does not provide for criminal sanctions.[79]

In a landmark 1969 case, *Tinker v. Des Moines School District,* the U.S. Supreme Court established that public schools cannot curtail students' freedom of speech unless this speech would cause a substantial disruption to school activities or violate the rights of other students.[80] Hence, a federal judge overturned the suspension of a high school senior who created a fake MySpace profile of his principal; the profile said the principal took drugs and kept alcohol at his desk. However, in a similar case, a U.S. district court ruled against a Pennsylvania junior high student who had created a fake MySpace profile of her principal claiming that he was a sex addict and a pedophile. She had been suspended for 10 days, and her parents sued the school. Teachers at the school testified that the profile had caused a disruption in class because students were too busy talking about the profile to pay attention in class. The court determined that the talking had constituted a "substantial disruption." Both of these decisions were upheld on appeal.[81]

Many states have recently enacted bullying laws that restrict written and symbolic speech on social media sites. In 2005, a Florida honors student committed suicide after three years of teasing at school and online bullying. As a result, in 2008, the state enacted a tough law called

the "Jeffrey Johnston Stand Up for All Students Act."[82] The law prohibits the teasing; social exclusion; threat; intimidation; stalking; sexual, religious, or racial harassment; or public humiliation of any public school student or employee on or offline. The law is limited in that it only applies to behavior during school, on a school bus, during any school-related or school-sponsored program or activity, or from computers that are part of a K-12 system.[83]

In January 2011, two Florida teenagers, Taylor Wynn and McKenzie Barker, were arrested for allegedly setting up a false Facebook account for a classmate that included nude photos. The teenage girls are accused of doctoring photographs, placing the classmate's face on the bodies of naked men and women, and posting them to the site. Although the victim told the school resource officer that the teasing would eventually "go away," a parent of another student notified authorities. Investigators traced the IP addresses to Wynn and Barker and collected incriminating text messages and emails linking them to the false Facebook page. Wynn and Barker were charged with stalking a minor under the new Jeffrey Johnston Stand Up for All Students Act.[84]

In another example of how serious online cyberbullying can get, 14-year-old Kameron Jacobsen, a freshman at Monroe-Woodbury High School in Orange County, New York, committed suicide after being taunted on Facebook for his presumed sexual orientation.[85]

Although freedom of speech is a right guaranteed by the U.S. Constitution, it can be restricted where it violates the other rights of individuals—as established by state or federal laws. To date, thirty-one states have antibullying laws that include electronic forms of bullying.[86]

Discussion Questions

1. Why is Facebook protected from liability for content posted by third parties? Do you think that Facebook and other social network providers should be protected from liability for what their members post? Why or why not?
2. How is a student's freedom of speech restricted on social media sites such as Facebook?
3. Should Taylor Wynn and McKenzie Barker have been prosecuted despite the victim's attitude that the teasing would pass? How should cyberbullying laws be implemented?

End Notes

1 "Best Reputation Management Company (ies) – March 2013," TopSEOS, www.topseos.com/rankings-of-best-reputation-management-companies (accessed March 7, 2013).

2 Reputation Changer, "Case Studies," www.reputationchanger.com/case_studies.html (accessed March 7, 2013).

3 Grant Schulte and Chet Brokaw, "'Pink Slime' Lawsuit: Defamation Case Against ABC News Tough to Prove, Experts Say," *Huffington Post*, September 14, 2012, www.huffingtonpost.com/2012/09/14/pink-slime-lawsuit-abc-news_n_1883528.html.

4 Martha Graybow, "ABC News Seeks Dismissal of Beef Products' Defamation Lawsuit," Reuters, November 1, 2012, http://uk.reuters.com/article/2012/11/01/usa-beef-pinkslime-abclawsuit-idUKL1E8LVHMI20121101.

[5] 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.

[6] *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.cornell.edu/supct/html/96-511.ZS.html (accessed January 26, 2013).

[7] Traverse Legal, "Section 230 of Communications Decency Act Does Not Provide An Absolute Immunity," July 2, 2009, http://section230communicationsdecencyact1996.com.

[8] Amanda Lee Myers, "Blogger Protests Ex-Cheerleaders Libel," *Yahoo!*, January 23, 2013, http://news.yahoo.com/blogger-contests-ex-cheerleaders-libel-suit-221705235–spt.html.

[9] Title XIV—Child Online Protection Act, Electronic Privacy Information Center, http://epic.org/free_speech/censorship/copa.html (accessed January 26, 2013).

[10] *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).

[11] Joel Engardio, "Internet Filters, Voluntary OK, Not Government Mandate," *Blog of Rights,* American Civil Liberties Union, January 26, 2009, www.aclu.org/2009/01/26/internet-filters-voluntary-ok-not-government-mandate.

[12] "2013 Best Internet Filter Software Reviews and Comparisons," *Top Ten Reviews,* http://internet-filter-review.toptenreviews.com (accessed January 26, 2013).

[13] "About Clearsail/Family.net, www.clearsail.net/about.htm (accessed January 26, 2013).

[14] Federal Communications Commission, "Children's Internet Protection Act: FCC Consumer Facts," www.fcc.gov/cgb/consumerfacts/cipa.html (accessed January 26, 2013).

[15] *United States v. American Library Association,* Supreme Court Online, Duke Law, www.law.duke.edu/publiclaw/supremecourtonline/editedcases/univame.html (accessed January 26, 2013).

[16] 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.

[17] Abraham Hyatt, "Enemies of the Internet: Not Just for Dictators Anymore," *ReadWriteWeb,* March 11, 2010, www.readwriteweb.com/archives/enemies_of_the_internet_not_just_for_dictators_anymore.php.

[18] 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).

[19] Maria Aguirre, "Cuba: Internet Censorship and a Generation That Has Never Spoken," *ICTs for the Bottom of the Pyramid* (blog), http://ict4bop.wordpress.com/2012/04/03/cuba-internet-censorship-and-a-generation-that-has-never-spoken, posted April 3, 2012.

[20] Abraham Hyatt, "Enemies of the Internet: Not Just for Dictators Anymore," *ReadWriteWeb,* March 11, 2010, www.readwriteweb.com/archives/enemies_of_the_internet_not_just_for_dictators_anymore.php.

[21] Lance Whitney, "Report Names Enemies of the Internet," *CNET,* March 15, 2010, http:// news.cnet.com/8301-13578_3-10468332-38.html.

[22] First Amendment Project, "Guarding Against the Chill: A Survival Guide for SLAPP Victims," www.thefirstamendment.org/antislappresourcecenter.html (accessed January 27, 2013).

[23] First Amendment Project, "The Anti-SLAPP Resource Center," www.thefirstamendment.org/antislappresourcecenter.html (accessed January 11, 2013).

[24] Evan Mascagni, "Will Lawsuit Muzzle Free Speech," Public Participation Project, January 11, 2013, www.anti-slapp.org/recent/will-lawsuit-muzzle-free-speech.

[25] "So What Is An Anti-SLAPP Law?," SLAPP'ed in Texas.com, April 1, 2011, http://slappedintexas.com/2011/04/01/so-what-is-an-anti-slapp-law.

[26] "So What Is An Anti-SLAPP Law?," SLAPP'ed in Texas.com, April 1, 2011, http://slappedintexas.com/2011/04/01/so-what-is-an-anti-slapp-law.

[27] Aaron Morris, "An Employee's Report to Human Resources is Protected by SLAPP Law," California SLAPP Law, January 12, 2013, http://californiaslapplaw.com/2013/01/an-employees-report-to-human-resources-is-protected-by-slapp-statute.

[28] 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.

[29] Janet Davison, "Online Vigilantes: Is 'Doxing' A Neighbourhood Watch or Dangerous Witch Hunt?", *CBC News*, October 22, 2012, www.cbc.ca/news/technology/story/2012/10/19/f-doxing-tracking-online-identity-anonymity.html.

[30] Christina Ng, "Bullied Teen Leaves Behind Chilling YouTube Video," *ABC News*, October 12, 2012, http://abcnews.go.com/International/bullied-teen-amanda-todd-leaves-chilling-youtube-video/story?id=17463266&page=1.

[31] "Amanda Todd's Tormenter Named by Hacker Group," *CBC News*, October 15, 2012, www.cbc.ca/news/canada/british-columbia/story/2012/10/15/bc-amanda-todd-tormentor-anonymous.html.

[32] European Digital Rights, "FBI Seizure to Threaten Anonymity and Freedom of Speech," EDRi-gram, April 25, 2012, www.edri.org/edrigram/number10.8/fbi-seizure-server-remailer.

[33] Jennifer Preston, "Group Says It Has Ceased Bomb Threats on Campus," *New York Times*, April 24, 2012, www.nytimes.com/2012/04/25/us/group-says-it-has-ceased-bomb-threats-at-university-of-pittsburgh.html?_r=0.

[34] "PrePaid Legal v. Sturtz Case Archive," Electronic Frontier Foundation, http://w2.eff.org/Censorship/SLAPP/Discovery_abuse/PrePaid_Legal_v_Sturtz/?f=20010712_proposed_order.html (accessed January 26, 2013).

[35] *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).

[36] YouTube, "Terms of Service," www.youtube.com/t/terms (accessed March 11, 2013).

[37] YouTube, "YouTube Community Guidelines," www.youtube.com/t/community_guidelines (accessed March 11, 2013).

[38] "The Stats on Internet Pornography," Information2Share, December 12, 2012, http://information2share.wordpress.com/2012/12/12/the-stats-on-internet-pornography.

[39] 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).

[40] Jerry Ropelato, "Internet Pornography Statistics," *TopTenREVIEWS,* http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html#anchor2 (accessed January 31, 2013).

[41] *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).

[42] Eric Goldman, "Internet Obscenity Conviction Requires Assessment of National Community Standards—US v. Kilbride" *Technology & Marketing Law Blog,* October 30, 2009, blog.ericgoldman.org/archives/2009/10/internet_obscen.htm.

[43] "New Data Shows Continued Work Productivity Losses From Web Surfing," Internetsafety.com, August 10, 2010, www.internetsafety.com/press-what-filtering-can-save-your-business.php.

[44] "Sex and Tech: Results from a Survey of Teens and Young Adults," National Campaign to Prevent Teen and Unplanned Pregnancy, www.thenationalcampaign.org/sextech/PDF/SexTech_Summary.pdf (accessed January 31, 2013).

[45] Doug Gross, "Snapchat: Sexting Tool, Or the Next Instagram?," *CNN*, January 10, 2013, www.cnn.com/2013/01/03/tech/mobile/snapchat/index.html.

[46] 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.

[47] Tom Symonds, "Spam Text Messages Pair Are Fined £440,000," *BBC*, November 28, 2012, www.bbc.co.uk/news/technology-20528301.

[48] Ken Magill, "Porn CAN-SPAM Conviction Upheld," *Direct,* September 11, 2007, http://directmag.com/email/news/porn_can-spam_conviction/#.

[49] Yelp, "About Us," www.yelp.com/about (accessed January 16, 2013).

[50] Gregory Ferenstein, "Berkeley Study: Half Star Change in Yelp Rating Can Make or Break a Restaurant," *Tech Crunch*, September 2, 2012 http://techcrunch.com/2012/09/02/berkeley-study-half-star-change-in-yelp-rating-can-make-or-break-a-restaurant/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Techcrunch+%28TechCrunch%29.

[51] Slander Defamation.com, "Dealing with Yelp," www.slanderdefamation.com/2012/03/26 (accessed January 16, 2013).

[52] Leena Rao, "Class Action Lawsuits Alleging Extortion Over Yelp's Review System Dismissed," *Tech Crunch*, October 26, 2011, http:\\techcrunch.com/2011/10/26/class-action-lawsuits-over-yelps-review-system-dismissed.

[53] Gregory Ferenstein, "Yelp Reviewer Gets SLAPPed with 750K Lawsuit and Order to Alter Comments," *Tech Crunch*, December 7, 2012, http://techcrunch.com/2012/12/07/yelp-reviewer-gets-slapped-with-750k-lawsuit-and-takedown-order.

[54] Chris Welch, "Judge Orders Woman To Tone Down Yelp Review As $750,000 Defamation Suit Heads To Court," December 7, 2012, www.theverge.com/2012/12/7/3740932/jane-perez-yelp-defamation-lawsuit.

[55] WikiLeaks, "About: What is WikiLeaks," http://wikileaks.org/About.html (accessed February 27, 2013).

[56] Joshua Hersh, "WikiLeaks Secret Diplomatic Cables Released In Full," *Huffington Post*, September 2, 2011, www.huffingtonpost.com/2011/09/02/wikileaks-diplomatic-cables_n_946574.html.

[57] Mark Mazzetti, "U.S. Expands Role of Diplomats in Spying," *New York Times*, November 28, 2010, www.nytimes.com/2010/11/29/world/29spy.html?_r=0.

[58] Frances Romero, "No More Secrets: The WikiLeaks War Logs," November 29, 2010, www.time.com/time/specials/packages/article/0,28804,2006558_2006562_2006567,00.html.

[59] Associated Press, "WikiLeaks Releases Largest Leak in U.S. History," *ABC News*, October 22, 2010, http://abclocal.go.com/wtvg/story?section=news/national_world&id=7741331.

[60] "A WikiLeaks Timeline," *The National Post*, November 28, 2010, http://news.nationalpost.com/2010/11/28/a-wikileaks-timeline.

[61] Susan Welch, John Gruhl, John Comer, Susan Rigdon, and Margery Abrosius, Understanding American Government, Wadsworth, 2001.

[62] Brian Bennett, "Bradley Manning Trial in WikiLeaks Case Delayed by Military Judge," *Los Angeles Times*, January 10, 2013, www.latimes.com/news/nation/nationnow/la-na-nn-wikileaks-manning-military-judge-20130110,0,2800502.story.

[63] David Leigh and Rob Evans, "WikiLeaks Says Funding Has Been Blocked After Government Blacklisting," *The Guardian*, October 14, 2010, www.guardian.co.uk/media/2010/oct/14/wikileaks-says-funding-is-blocked.

[64] Gregg Keizer, "WikiLeaks Moves to Amazon Servers After DoS Attacks," *Computerworld*, November 29, 2010, www.computerworld.com/s/article/9198418/WikiLeaks_moves_to_Amazon_servers_after_DoS_attacks.

[65] Patrick Thibodeau, "With WikiLeaks, Amazon Shows Its Power Over Customers," *Computerworld*, December 2, 2010, www.computerworld.com/s/article/9199258/With_WikiLeaks_Amazon_shows_its_power_over_customers.

[66] Ravi Somaiya, "Hundreds of WikiLeaks Mirror Sites Appear," *New York Times*, December 5, 2010, www.nytimes.com/2010/12/06/world/europe/06wiki.html?_r=2.

[67] Arthur Bright, "WikiLeaks' Julian Assange Arrested in London on Rape Charges," *Christian Science Monitor*, December 7, 2010, www.csmonitor.com/World/terrorism-security/2010/1207/WikiLeaks-Julian-Assange-arrested-in-London-on-rape-charges.

[68] "Julian Assange Fast Facts," *CNN*, January 18, 2013, www.cnn.com/2013/01/18/world/julian-assange-fast-facts.

[69] Kevin Poulsen and Kim Zetter, "Threat Level: Will 400,000 Secret Iraq War Documents Restore WikiLeaks' Sheen?" *Wired*, October 15, 2010, www.wired.com/threatlevel/2010/10/wikileaks-iraq.

[70] Raffi Khatchadourian, "No Secrets: Julian Assange's Mission for Total Transparency," *New Yorker*, June 7, 2010, www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian?currentPage=1.

[71] Raffi Khatchadourian, "No Secrets: Julian Assange's Mission for Total Transparency," *New Yorker*, June 7, 2010, www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian?currentPage=1.

[72] WikiLeaks, www.wikileaks.org (accessed January 20, 2013).

[73] David Ardia, "Finkel v. Facebook: Court Rejects Defamation Claim Against Facebook Premised on 'Ownership' of User Content," Citizen Media Law Project (blog post), October 21, 2009, www.citmedialaw.org/blog/2009/finkel-v-facebook-court-rejects-defamation-claim-against-facebook-premised-ownership-user-.

[74] Chris Matyszczyk, "Teen Sues Facebook, Classmates over Cyberbullying," *CNET,* March 3, 2009, http://news.cnet.com/8301-17852_3-10187531-71.html.

[75] Title 47, Chapter 5, Subchapter II, Part I, § 230, "Protection for Private Blocking and Screening of Offensive Material," Legal Information Institute, Cornell University Law School, www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000230——000-.html (accessed February 22, 2011).

[76] Supreme Court of the State of the New York Count of New York, *Denise E. Finkel, Plaintiff against Facebook, Inc., Michael Dauber, Jeffrey Schwarz, Melinda Danowitz, Leah Herz, Richard Dauber, Amy Schwartz, Elliot Schwartz, Martin Danowitz, Bari Danowitz, Alan Herz, and Ellen Herz, Defendants,* Affirmation in Opposition, Index No. 101578-09, www.citmedialaw.org/sites/citmedialaw.org/files/2009-03-26-Finkel%20Opposition%20to%20Facebook%20Motion%20to%20Dismiss.pdf (accessed February 22, 2011).

[77] *Finkel v. Facebook,* Citizen Media Law Project, www.citmedialaw.org/threats/finkel-v-facebook (accessed February 22, 2011).

[78] *Finkel v. Facebook,* Citizen Media Law Project, www.citmedialaw.org/threats/finkel-v-facebook (accessed February 22, 2011).

[79] Sameer Hinduja and Justin W. Patchin, "State Cyberbullying Laws: A Brief Review of State Cyberbullying Laws and Policies," Cyberbullying Research Center, www.cyberbullying.us/Bullying_and_Cyberbullying_Laws.pdf (accessed February 23, 2011).

[80] *Tinker v. Des Moines School Dist.,* 393 U.S. 503 (1969), First Amendment Center, www.firstamendmentschools.org/freedoms/case.aspx?id=404 (accessed February 23, 2011).

[81] David Kravets, "Rulings Leave Online Student Speech Rights Unresolved." *Wired,* February 4, 2010, www.wired.com/threatlevel/2010/02/rulings-leave-us-student-speech-rights-unresolved.

[82] "I Couldn't Get Them to Stop," Polk County Public Schools, www.polk-fl.net/parents/generalinformation/documents/bullyingjeffreyjohnstonstory.pdf (accessed February 24, 2011).

[83] The 2010 Florida Statutes, 1006.147 "Bullying and Harassment Prohibited," Online Sunshine, The Florida Legislature, www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=1000-1099/1006/Sections/1006.147.html (accessed February 24, 2011).

[84] Amar Toor, "Teens Arrested for Cyberbullying Classmate with Fake Facebook Profile, Nude Photos," *Switched,* January 14, 2011, www.switched.com/2011/01/14/fake-facebook-profile-cyberbullying-gets-teens-arrested/.

[85] Lisa Evers, "Sources: Teenager Kills Himself After Facebook Taunts," *Fox 5 News,* January 19, 2011, www.myfoxny.com/dpp/news/local_news/new_york_state/sources-teenager-kills-himself-after-facebook-taunts-20110119.

[86] Sameer Hinduja and Justin W. Patchin, "State Cyberbullying Laws: A Brief Review of State Cyberbullying Laws and Policies," Cyberbullying Research Center, www.cyberbullying.us/Bullying_and_Cyberbullying_Laws.pdf (accessed February 25, 2011).

CHAPTER 6

INTELLECTUAL PROPERTY

QUOTE

Intellectual property has the shelf life of a banana.
—Bill Gates, founder of Microsoft

VIGNETTE

Sinovel Steals Millions in Trade Secrets from American Superconductor

In 2006, the Chinese government passed a clean air energy law that mandated the creation of seven giant wind farms, each of which would, within a decade and a half, produce as much energy as 10 nuclear reactors. Daniel McGahn, vice president in charge of new business for American Superconductor (AMSC), saw a tremendous opportunity for his company in China. Over the course of the next several years, AMSC made deals with several Chinese companies that would manufacture wind turbines for which AMSC would supply the electronic control systems, the software, and the electrical components necessary to transform the wind energy generated into electrical power.[1] And for a while, that strategy paid off.

AMSC produces advanced smart grid technology for power companies and electronic control systems that maximize wind turbine reliability, availability, and energy output. Yet American power companies have been reluctant to update their systems with smart grid technology that could prevent outages simply because of the huge cost involved in such an investment.[2] So, the Chinese

wind legislation was a windfall for AMSC. AMSC stock quadrupled in value between 2006 and 2009.[3]

AMSC's largest customer in China was Sinovel Wind Group, a company that had bid on and won 47 percent of the Chinese government's wind projects. Sinovel captured a leading position in China's wind market. However, as more and more Chinese companies began producing turbines, the price of turbines dropped by 40 percent, and Sinovel's profits also dropped. Still, AMSC had multiyear contracts with Sinovel at set prices, and Sinovel continued to produce large quantities of turbines equipped with AMSC technology.

In March 2011, Sinovel began rejecting AMSC shipments of electronic components—shipments worth more than $70 million—without explanation. In April of that year, AMSC was forced to announce that Sinovel had stopped placing orders, despite the fact that AMSC had contracts committing Sinovel to $700 million in future orders. Daniel McGahn, now CEO of AMSC, tried to uncover the problem and mend relations, but Sinovel declined to resume placing orders. Then, in June 2011, a group of AMSC engineers testing a Sinovel turbine in northern China uncovered electrical components that were running a stolen version of AMSC software. Sinovel had somehow accessed AMSC proprietary source code and was manufacturing its own electrical components, cutting AMSC out of the operation.[4]

In 2010 and 2011, China had experienced major disruptions in its power grids as disturbances, such as trees falling on lines, shut down thousands of turbines. The Chinese government proposed legislation to require energy companies such as Sinovel to upgrade their electrical components with software that would allow wind farms to continue to function despite power grid disturbances. Because AMSC software controlled all of Sinovel's existing turbines, Sinovel would be required to

purchase the software upgrade from AMSC.[5] Instead, Sinovel recruited an Austrian-based AMSC engineer, Dejan Karabasevic, to develop the necessary software. Sinovel signed an employment contract with Karabasevic and flew him to an apartment in Beijing, along with code stolen from AMSC's servers in Austria. He then spent several weeks reverse engineering the software to come up with the source code necessary to install in Sinovel's turbines.

After AMSC discovered the stolen software, the company was able to track it back to Karabasevic. Ultimately, Karabasevic confessed to Austrian police and was sentenced to 12 months in prison for revealing trade secrets.[6] AMSC filed several lawsuits against Sinovel in Chinese courts, seeking $1.2 billion in damages for intellectual property theft and breach of contract, while Sinovel has countersued for $207 million, claiming AMSC provided substandard quality equipment. The court battle, which garnered the attention of top U.S. and Chinese officials, is seen as a test case. Many Western companies (including DuPont, Google, and Lockheed Martin) have claimed that they have been victims of Chinese espionage, and the court's decision will be an indication of whether China is willing to restrict such behavior.[7] China's Supreme Court surprised many when it agreed to review lower court decisions dismissing one of AMSC's claims.[8]

The director of the National Security Agency has called the theft of technological secrets by Chinese companies from U.S. and Western companies "the greatest transfer of wealth in history."[9] American leaders perceive these cases not as isolated incidents, but rather as part of a larger strategy of employing unfair trading practices—similar to China's decision to corner the market on rare earth metals needed to produce high-tech hardware. The U.S. International Trade Commission has estimated that if China instituted intellectual property protection measures similar to those in the United States, the United States would gain between 900,000 and 2.1 million jobs.[10] Yet AMSC and many other Western companies continue to do business in China.

AMSC is still working to recover from its 2011 losses when its stock dropped from almost $30 to $4 per share. The company has signed deals in Korea, India, and Russia for its electrical control systems, and Daniel McGahn recently noted that "silver linings are beginning to appear" as China is forecasting an increase in wind turbine installations now that stricter quality regulations have been implemented.[11]

Questions to Consider

1. What additional evidence would convince you that China's theft of technological secrets represents a national strategy rather than just a series of isolated incidents?
2. What actions might Western countries take to protect the loss of technological secrets and to reduce the risk of continuing to do business in China?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What does the term *intellectual property* encompass, and why are organizations so concerned about protecting intellectual property?
2. What are the strengths and limitations of using copyrights, patents, and trade secret laws to protect intellectual property?
3. What is plagiarism, and what can be done to combat it?
4. What is reverse engineering, and what issues are associated with applying it to create a lookalike of a competitor's software program?
5. What is open source code, and what is the fundamental premise behind its use?
6. What is the essential difference between competitive intelligence and industrial espionage, and how is competitive intelligence gathered?
7. What is cybersquatting, and what strategy should be used to protect an organization from it?

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. Intellectual property 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 legislation 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."[12] 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, 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.[13]

These extensions were primarily championed by movie studios concerned about retaining rights to their early films. Opponents argued that lengthening 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.[14]

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. 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 Ronald Mack and recorded by the Chiffons in 1962.[15]

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. The fair use doctrine 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:

- The purpose and character of the use (such as commercial use or nonprofit, educational purposes)
- The nature of the copyrighted work
- The portion of the copyrighted work used in relation to the work as a whole
- The effect of the use on the value of the copyrighted work[16]

The concept that an idea cannot be copyrighted but the expression of an idea can be is 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.

The HathiTrust Digital Library is a joint project involving major research institutions, the libraries of several universities, and Google. The intent of the project was for Google to create a searchable database of the holdings of the participants, along with tools to facilitate access and searching of the database.[17] However, in 2011, the Authors Guild, an advocacy group for writers, filed a lawsuit alleging the project violated copyright law because the process of creating and accessing the digital library involved the unauthorized creation of multiple copies of the books. HathiTrust argued that its use of the material was "transformative" and thus permissible under conditions of the fair use doctrine. In this situation, a transformative act is one in which enough new material is added to a work to change the nature of the work or to modify the purpose for which the work is intended. The judge in the case reasoned that scanning and indexing the books for the purpose of allowing readers to search the content was indeed transformative and ruled in favor of HathiTrust.[18,19]

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.

Tetris is a very popular computer game that was created in 1984. Over the years, versions of Tetris have been developed and licensed to run on Nintendo's Game Boy, DS, and Wii; Sony's PlayStation; Apple's iPod, iTouch, and iPhone; and Android phones.[20] Xio Interactive was a small company formed for the purpose of creating an unlicensed iPhone version of Tetris—named Mino.[21] However, shortly after Xio posted its Mino app to the Apple iTunes store, Tetris filed a copyright infringement lawsuit against the company. In its defense, Xio argued that because it only copied the rules and basic functionality of the game, and not its more original components, there was no infringement. While the court agreed that the fundamental rules and basic functionality of the game could not be protected, it pointed out that many other elements of the game had been copied, including the color, shape, and number of game bricks; how the pieces were formed from the game bricks; and the manner in which the pieces moved. In addition, the court noted that screen shots of the games viewed side by side were nearly

identical. The court ruled that Xio was permanently banned from selling, displaying, or promoting the Mino game.[22]

The Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008

The **Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008** increased trademark and copyright enforcement and substantially increased penalties for infringement. For example, the penalty for infringement of a 10-song album was raised from $7,500 to $1.5 million. The law also created the Office of the United States Intellectual Property Enforcement Representative within the U.S. Department of Justice. One of its programs, called CHIP (Computer Hacking and Intellectual Property), is a network of over 150 experienced and specially trained federal prosecutors who focus on computer and intellectual property crimes.[23]

General Agreement on Tariffs and Trade (GATT)

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. 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 World Trade Organization (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 WTO is headquartered in Geneva, Switzerland, and had 158 member nations as of February 2013. The goal of the WTO is to help producers of goods and services, exporters, and importers conduct their business.[24]

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 Line: World Trade Organization, "Overview: The TRIPS Agreement," www.wto.org/english/tratop_e/trips_e/intel2_e.htm.

The World Intellectual Property Organization (WIPO) 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.[25]

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 U.S. law through the Digital Millennium Copyright Act (DMCA), which is discussed in the next section.

The Digital Millennium Copyright Act (1998)

The **Digital Millennium Copyright Act (DMCA)** 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:

- *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 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.

- *Title II (Online Copyright Infringement Liability Limitation Act)*—This section enables Web site operators that allow users to post content on their Web site (e.g., music, video, and pictures) to avoid copyright infringement liability if certain "safe harbor" provisions are followed.
- *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.
- *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.
- *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 (shown in Figure 6-1) 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 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

FIGURE 6-1 Several cases brought under the DMCA have dealt with the use of software to enable the copying of DVD movies

Credit: © Polat/Shutterstock.com

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 infringers identified through their ISP. Title II of the DMCA also provides defined procedures for ISP users to challenge improper takedowns.

The takedown procedure works as follows. The owners of copyrighted material who allege that their material has been infringed send a notice to the ISP hosting the content. The ISP forwards the notice to whoever was responsible for uploading material. That individual is given a chance to respond. If there is no response, the ISP must ensure that the material is no longer accessible. The ISP forfeits its protection under the safe harbor conditions if it fails to remove the material in a prompt manner.

Because many copyright infringers take measures to conceal their true identity, copyright owners 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.

Viacom International filed a $1 billion copyright infringement lawsuit against YouTube and its parent company Google in March 2007. Viacom alleged that YouTube violated the DMCA by permitting its users to post copyright-protected material from Viacom's various networks and subsidiaries—including Comedy Central, MTV, BET, and Paramount Pictures—without permission. Initially, a district court ruled that YouTube was immune from copyright liability because it was protected by the safe harbor provisions of the DMCA, even though Viacom had argued that YouTube had a "general awareness" of widespread infringement, which should disqualify YouTube from safe harbor protections.[26] Upon

appeal, the Second Circuit Court of Appeals determined that internal email exchanges among YouTube employees suggested that YouTube may have had specific knowledge of some infringing film clips. In April 2012, the Second Circuit Court of Appeals reinstated Viacom's lawsuit, and ordered the district court to reexamine the case to determine if YouTube is entitled to DMCA safe harbor protection.[27]

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."[28]

PATENTS

A **patent** is a grant of a property right issued by the United States 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. Figure 6-2 shows the number of patents applied for and granted in recent years.

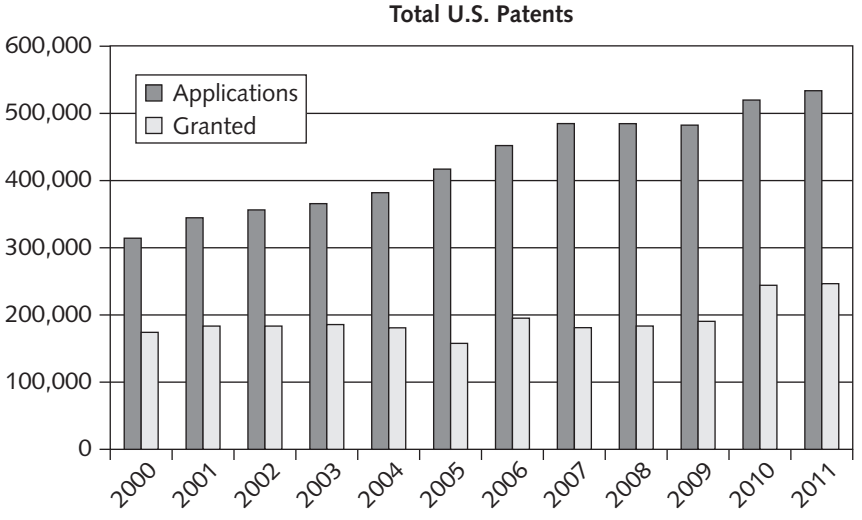


FIGURE 6-2 Patents applied for and granted
Source Line: U.S. Patent Statistics Calendar Years 1963–2011, www.uspto.gov/web/offices/ac/ido/oeip/taf/us_stat.pdf.

IBM obtained 6,478 patents in 2012, the 20th consecutive year it received more patents than any other company in the United States.[29] By some estimates, IBM's licensing of patents and technologies generates several hundred million dollars in annual revenue for the company.[30] Table 6-2 lists the IT organizations that were granted the most patents in 2012.

TABLE 6-2 IT organizations that received the most patents in 2012

Organization	Number of patents granted	Increase over 2011
IBM	6,478	5%
Samsung	5,081	4%
Canon	3,174	12%
Microsoft	2,613	13%[31]
Google	1,151	170%
Apple	1,136	68%

Source Line: "IBM Top Patent Producer 20 Years Running," *CNM Online*, January 13, 2013, www.cnmeonline.com/news/ibm-top-patent-producer-20-years-running.

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 7,800 patent examiners to research the originality of each patent application, the average time from filing until the application is issued as a patent or abandoned by the applicant is around 31 months as of January 2013. At the end of 2012, there was a backlog of 597,579 unexamined patent applications.[32] 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 which 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.

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 copyright infringement, there is no specified limit to 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.

Leahy-Smith America Invents Act (2011)

The **Leahy-Smith America Invents Act** represents a major change in U.S. patent law. Under this law, which was passed in 2011, the U.S. patent system changed from a "first-to-invent" to a "first-inventor-to-file" system effective 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.[33,34]

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.[35]

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.[36]

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.[37] 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.[38] Some software experts think that too many software patents are being granted, and they believe that this inhibits new software development.[39] Indeed, each new software patent lawsuit adds to the costs and business risks associated with

software development. During 2012, the following software patent battles were raging among some of the biggest names in the software industry:

- Oracle and Google battled over patent infringement claims associated with Oracle's Java programming language—with Oracle seeking $6 billion in damages.[40]
- Apple sued Samsung for patent infringement regarding several patents associated with Apple's smartphone and tablet devices. Apple was ultimately awarded $1.1 billion in damages.[41]
- Mformation, a global provider of mobile device management technology, was awarded $147 million when it sued Research in Motion for patent infringement of Mformation's patented technology, which enables companies to remotely access employee mobile phones to perform software upgrades, change passwords, and erase data.[42]
- Many industry observers believe that Google purchased Motorola Mobility, a smartphone software company, for $12.5 billion so that the firm could sue Apple over alleged infringement of patents associated with location reminders, email notification, and the Siri intelligent assistant.[43]

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, which eventually led to the U.S. International Trade Committee banning imports of two models of the HTC mobile phone. The two companies eventually agreed to a 10-year cross-licensing agreement that permits each party to license the other's current and future patents.[44]

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.[45]

TRADE SECRETS

In Chapter 2, a trade secret was 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.

Fuhu is the creator of Nabi, an Android tablet computer for kids, that had been sold exclusively at Toys "R" Us stores. In a lawsuit filed in late 2012, Fuhu alleged that Toys "R" Us stole Nabi trade secrets during the year that the retailer served as the exclusive distributor of the product. As a result, Fuhu alleged, Toys "R" Us was able to bring out its competing tablet months ahead of schedule. Fuhu sued to stop the toy retailer from launching this rival tablet during the lucrative Christmas selling season.[46]

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.

Uniform Trade Secrets Act (UTSA)

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.[47]

The Economic Espionage Act (EEA) (1996)

The **Economic Espionage Act (EEA) of 1996** 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 pursue economic espionage; the FBI was investigating nearly 800 such cases in 23 countries when the EEA was enacted.[48] The Office of the National Counterintelligence Executive has estimated that the "combined costs of foreign and domestic economic espionage, including the theft of intellectual property, [are] as high as $300 billion per year and rising."[49] As with the UTSA, information is considered a trade secret under the EEA only if companies take steps to protect it.

DuPont is a major U.S.-based science and engineering company that has been in business since 1802.[50] The firm was a leader in research on Organic Light Emitting Diodes (OLED) that resulted in the development of a breakthrough and proprietary chemical process for OLED displays. However, a DuPont research chemist involved in the project stole trade secret compounds and passed them to a Chinese university. Ultimately, the chemist was caught by the FBI, prosecuted, and sentenced to 14 months in federal prison. The loss of the trade secrets was valued by DuPont at $400 million.[51]

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.[52]

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 seldom enforced in California.[53]

Electronic payments processing firm Vantiv filed a lawsuit alleging breach of a noncompete contract against its former senior vice president when he accepted a position with competitor iPayments. Vantiv hopes to bar the employee from working for the competitor and to gain return of a year's base salary received as part an employment termination agreement.[54] In another case, five software engineers brought a class action lawsuit against Apple, Google, Intel, Adobe Systems, Intuit, Pixar, and Lucasfilm alleging that the firms colluded to constrain salary and job mobility by maintaining do-not-call lists to avoid recruiting each other's employees. The engineers alleged that these agreements restrained competition and potentially cost the employees of these firms hundreds of millions of dollars.[55]

The following is an example of a typical, although not necessarily 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.

KEY 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.[56] 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.[57]

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 6-3) allow teachers, corporations, law firms, and publishers to check for matching text in different documents as a means of identifying potential plagiarism.

TABLE 6-3 Partial list of plagiarism detection services and software

Name of service	Web site	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
EVE Plagiarism Detection	www.canexus.com/eve	CaNexus

Source Line: Course Technology/Cengage Learning.

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 24 billion Web pages, some 300 million archived student papers, and 120 million articles from over 110,000 journals, periodicals, and books.[58] 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.[59]

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 a 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."[60]

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 students aware that they know how to use these services.
- Incorporate detection software and services into a comprehensive antiplagiarism program.

Reverse Engineering

Reverse engineering is the process of taking something apart in order to understand it, build a copy of it, or improve it. Reverse engineering 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.[61]

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 (for example, 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, REC (Reverse Engineering Compiler) 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 open source code.[62]

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 smartphones and other mobile devices, such as Apple's iPhone, Palm's Treo, and Research In Motion's BlackBerry. See Table 6-4 for a listing of commonly used open source software.

TABLE 6-4 Commonly used open source software

Open source software	Purpose
7-Zip	File compression
Ares Galaxy	Peer-to-peer file sharing
Audacity	Sound editing and special effects
Azureus	Peer-to-peer file sharing
Blender 3D	3D modeling and animation
eMule	Peer-to-peer file sharing
Eraser	Erasing data completely
Firefox	Internet browsing
OpenOffice	Word processing, spreadsheets, presentations, graphics, and databases
Video Dub	Video editing

Source Line: Course Technology/Cengage Learning.

Why would firms or individual developers create open source code if they do not receive money for it? Here are several reasons:

- 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 composed 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 Web site, *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 (as defined in Chapter 3) 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. According to a recent survey of 400 global companies with competitive intelligence programs, the number of companies that spend more than $1 million on this activity increased from 5 percent to 10 percent over the period 2007–2012.

Pharmaceutical companies represent 27 percent of the companies that spend more than $2 million on competitive intelligence.[63]

Competitive intelligence is used to support smart business decisions in many different areas. For example, a European sporting goods manufacturer wanted to enter the U.S. market and was looking for good entry opportunities. Gathering and analyzing data about its competitors, the firm discovered an overlooked and rapidly growing market—wrestling headgear and apparel for girls.[64]

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 5 percent of common stock in a public company
- 10-Q or quarterly reports
- Press releases
- Promotional materials
- Web sites
- 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 a database of contract documents available online 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 Web site 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 6-5 provides a manager's checklist for running an ethical competitive intelligence operation. The preferred answer to each question in the checklist is *yes*.

TABLE 6-5 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 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?		

Source Line: Course Technology/Cengage Learning.

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, Chapter 22 of the U.S. Code) defines the use of a trademark, the process for obtaining a trademark from the Patent and Trademark Office, 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 Web site 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 where a defendant uses 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:[65]

- The plaintiff's product or service cannot be readily identifiable without using the plaintiff's mark.
- It uses only as much of the plaintiff's mark as necessary to identify the defendant's product or service.
- The defendant does nothing with the plaintiff's mark that suggests endorsement or sponsorship by the plaintiff.

This defense was first applied to Web sites in *Playboy Enterprises, Inc. v. Terri Welles.* Welles was the Playboy™ Playmate of the Year™ in 1981. In 1997, she created a Web site 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 *Playboy* model and *Playmate of the Year* to describe herself on her Web site. 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 Web site.[66]

IGB Eletronica is a Brazilian telecommunications firm that designs and markets various consumer electronics products, including smartphones, for the Brazilian market. In 2002, the firm petitioned the Brazilian Industrial Property Institute for the exclusive rights to the product name "iPhone." IGB was finally granted rights to the name in 2007, by coincidence, the same year that Apple's first iPhone was released. That same year, IGB launched the Gradiente iPhone, which runs the Android operating system. Apple initiated a lawsuit over IGB's use of the iPhone, which continued for the next six years.[67]

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 Web sites. When Web sites were first established, there was no procedure for validating the legitimacy of requests for Web site 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 (for example, 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.

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 Web site.

Ally Financial, a financial services company providing insurance, direct banking, and commercial financing services recently filed a lawsuit under the Anticybersquatting Consumer Protection Act against a man for allegedly registering three domain names that were very similar to domain names used by Ally. Ally customers who mistakenly visited those Web sites were redirected to VeteransNationalBank.us, a site owned by the defendant in the case. When Ally initially contacted the man to inform him of the bank's right to the domain names, he demanded that Ally work with him in some sort of new banking venture. Ally rejected the proposal, and the man modified his Web sites to redirect Web site visitors to an Ally competitor, Chase Bank. Ally is seeking damages of up to $100,000 per domain name.[68,69]

Summary

- *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; prepare derivative works based on the work; and grant these exclusive rights to others.
- 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 can 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 establishes 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) 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. It 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 United States Patent and Trademark Office 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: It must be useful; it must be novel; and it must not be obvious to a person having ordinary skill in the same field.
- 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 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.
- Unlike copyright infringement, for which monetary penalties are limited, 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 courts and the U.S. Patent and Trademark Office 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 and the Economic Espionage Act.
- 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.
- 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. Reverse engineering 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 refers to 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. Competitive intelligence 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. Web site 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
Digital Millennium Copyright Act (DMCA)
Economic Espionage Act (EEA) of 1996
fair use doctrine
industrial espionage
intellectual property
Leahy-Smith America Invents Act
noncompete agreement
nondisclosure clause
open source code
patent
patent infringement
plagiarism
prior art
Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008
reverse engineering
trademark

Self-Assessment Questions

The answers to the Self-Assessment Questions can be found in Appendix B.

1. Which of the following is an example of intellectual property?
   a. a work of art
   b. a computer program
   c. a trade secret of an organization
   d. all of the above

2. Copyright law protects authored works; _____ law protects inventions.
3. Software can be protected under copyright law, but it can also be patented. True or False?
4. The courts may award up to triple damages for which of the following?
   a. patent infringement
   b. copyright infringement
   c. trademark infringement
   d. theft of trade secrets
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 copyright infringement. True or False?
6. Title II of the _____ amends the Copyright Act by adding a new section that enables a Web site operator that allows users to post content on its Web site 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 WTO developed the _____, which established minimum levels of protection that each government must provide to the intellectual property of all WTO members.
12. Plagiarism is an issue only in academia. 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. Almost all the data needed for competitive intelligence can be collected either through carefully examining published information or through interviews. True or False?

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.

Discussion Questions

1. 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.
2. Briefly discuss Title I and II of the DMCA, including the primary protections it provides for copyright material as well as the associated penalties. Do you believe that the DMCA has given excessive powers to copyright holders? Why or why not?
3. Identify the necessary conditions to grant a patent according to Title 35 of the U.S. Code.
4. How did the America Invents Act modify U.S. patent law? Do you think this act was an improvement over the preexisting way of patenting? Why or why not?
5. What is a cross-licensing agreement? How do large software companies use such agreements? Do you think their use is fair to small software development firms? Why or why not?
6. What is the role of the WTO, and what is the scope and intent of its TRIPS agreement?
7. 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?
8. 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?
9. What problems can arise in using nondisclosure and noncompete agreements to protect intellectual property?
10. Outline a multistep approach that a university might take to successfully combat plagiarism among its students.
11. Under what conditions do you think the use of reverse engineering is an acceptable business practice?
12. How might a corporation use reverse engineering to convert to a new database management system? How might it use reverse engineering to uncover the trade secrets behind a competitor's software?
13. Why might an organization elect to use open source code instead of proprietary software?
14. What is the nominative use defense? What are the three key elements of this defense?
15. What measures can companies take to combat cybersquatting?

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 have been asked to lead your company's new competitive intelligence organization. What would you do to ensure that members of the new organization obey applicable laws and the company's own ethical policies?
2. You are interviewing for the role of human resources manager for a large software developer. 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?
3. You have been asked by the manager of software development to lead a small group of software developers in an attempt to reengineer the latest release of the software by your leading competitor. The goal of the group is to identify features that could be implemented into the next few releases of your firm's software. You are told that the group would relocate from the United States to the island of Antigua, in the Caribbean Sea, to "reduce the risk of the group being distracted by the daily pressures associated with developing fixes and enhancements with the current software release." What sort of legal and/or ethical questions might be raised by this reengineering effort? Would you consider taking this position?
4. You have procrastinated too long and now your final paper for your junior English 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 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" Web sites, 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?
5. Your friend is a two-time winner of the Ironman™ Arizona Triathlon (2.4-mile swim, 112-mile bike, and 26.2-mile run). He is also a popular and well-known marathon runner throughout the Southwest. He has asked you to design a Web page to promote the sale of a wide variety of health products, vitamins, food supplements, and clothing targeted at the athletes training to participate in the triathlon. The products will carry his personal trademark. However, much of the information on the Web page will include discussion of his personal success in various triathlons and marathons in which he has competed. Many of these events have corporate sponsors and carry their own trademark. He has asked you if there are any potential trademark issues with his marketing plans. What would you do?
6. You are beginning to feel very uncomfortable in your new position as a computer hardware salesperson for a firm that is the major competitor of your previous employer. Today, for the second time, someone has mentioned to you how valuable it would be to know what the marketing and new product development plans were of your exemployer.

You stated that you are unable to discuss such information under the nondisclosure contract signed with your former employer, but you know your response did not satisfy your new coworkers. You fear that the pressure to reveal information about the plans of your former company is only going to increase over the next few weeks. What do you do?

7. Because of the amount of the expense, your company's CFO had to approve a $500,000 purchase order for hardware and software needed to upgrade the servers used to store data for the Product Development Department. Everyone in the department had expected an automatic approval, and they were disappointed when the purchase order request was turned down. Management said that the business benefits of the expenditure were not clear. Realizing that she needs to develop a more solid business case for the order, the vice president of product development has come to you for help. Can you help her identify arguments related to protecting intellectual property that might strengthen the business case for this expenditure?
8. 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. Which option would you pursue and why?

Cases

1. Alice Case Raises Concerns for the Future of IT Software Patents

On February 8, 2013, the Federal Circuit Court of Appeals met to consider a case that could shape the future of technology innovation in the United States. The case involved the Alice Corporation, an Australian company that obtains financial market patents from the United States, the United Kingdom, and other major trading nations.[70] Alice holds four patents for a business method that CLS Bank International employs to reduce risk in financial transactions. In 2007, Alice sued CLS Bank International and other companies for patent infringement, hoping to reap financial gain. CLS Bank, however, countersued Alice claiming that Alice's patents were in violation of Section 101 of the Patent Act.

Section 101 states that the U.S. government cannot grant patents for "laws of nature, natural phenomena, and abstract ideas."[71] Rather, patents must involve only practical applications of abstract ideas. But what is the difference between an abstract idea and a practical application? The answer to this question involves high stakes—billions of dollars in the IT industry.

Many lawyers who represent IT companies describe patent-enforcing companies (such as Alice Corporation) as "patent trolls." Such companies do not produce a product themselves. Rather patent trolls make money by threatening to sue technology companies that supposedly make use of their patented ideas. The patent troll is usually not the inventor, but rather a company that has purchased patents from bankrupt technology companies, usually failed start-ups.

Patent trolls generally target companies with annual revenues between $50 and $200 million. These companies are large enough to pay licensing fees, but often lack resources to pay steep litigation fees.[72]

For example, a company called Ultramercial obtained a patent for the idea of "pre-roll advertisements"—ads placed prior to the broadcasting of free video clips broadcast on YouTube and Hulu. These ads are a major revenue source for YouTube, Hulu, and other companies. One of these companies, Wild Tangent, sued Ultramercial asserting that its patent claim was invalid; however, an appellate court upheld a lower court's ruling declaring the patent valid.[73] In the summer of 2012, the Supreme Court issued a ruling in the case asking the appellate court to reconsider its ruling, which, if not overturned, would force companies such as YouTube and Hulu to pay large licensing fees to Ultramercial.

According to Google general council Kent Walker, "Abuses of our patent system cost the economy $29 billion in 2011, raising prices and reducing choice. Technology moves incredibly fast, and the United States Patent and Trademark Office need to take prompt action."[74]

Software patents were not even recognized by U.S. Courts until the *States Street* case of 1998. Up to that point, many companies had patented software ideas for business methods, but none of the patents had been enforced.[75] In 1998, the U.S. Court of Appeals recognized Signature Financial Group's patent of a business method using computers and allowed the company to collect licensing fees from States Street Bank.

Since the *States Street* decision, the U.S. court system has been floundering with the issue. Different courts have come down on different sides. In the earlier appellate hearing of the Alice case, two judges of the three-judge panel held for Alice Corporation and argued for an extraordinarily broad interpretation of patent law. Now, most of the heavyweights of the U.S. IT sector—Google, IBM, Facebook, Intel, and others—have filing *amicus* briefs, legal opinions in support of one side or the other. IBM, which has led the world in number of new patents for 21 years, filed a brief in support of Alice. Google and Facebook, which are leading product producers, filed in support of CLS Bank. Intel, a computer chip manufacturer that has many patents but is fearful of the large number of patents in the field of theoretical chip design, also filed on the side of the bank.[76]

The new appellate court decision will likely pave the way for the Supreme Court to weigh in on the matter more extensively. A decision in favor of Alice would mean an explosion of patent litigation and increase in costs for IT producers. A decision against Alice would be a boost for large IT software manufacturers and creators on online content and products who may be less careful about paying licensing fees to small patent holders. The Department of Justice has filed an *amicus* brief favoring neither side. Instead, the department has called on the appellate court not to issue a decision that would create a hard-and-fast rule, but that would allow the courts to consider each case individually.[77] This action indicates that the U.S. government feels that both positions have some merit. On the one hand, patent trolls are reducing U.S. productivity. On the other hand, the Department of Justice recognizes the need to protect the owners of intellectual property.

Discussion Questions

1. How unique does an idea need to be to warrant patent protection? Should the idea of pre-roll advertisements be patentable?

2. Are patent trolls justified in their actions? Do they provide a means of rewarding small innovators?
3. Are patent lawsuits likely to decrease or increase innovation in the United States?

2. Rockstar Consortium—Beware the Patent Troll

Nortel was a Canadian multinational telecommunications and data network equipment manufacturing pioneer. Nortel patented many innovations in the areas of wireless communications, telecommunications switching, Internet routers, modems, personal computers, search, and social networking.[78] Many of its patents are in the key areas of Long Term Evolution (LTE) and 3G technologies, which are the foundation of modern wireless networks.[79]

In 2009, Nortel filed for bankruptcy, and in the process, the company sold its business units and assets to various purchasers.[80] Approximately 6,000 of its patents were sold for $4.5 billion to a company formed by a team of information technology companies consisting of Apple, EMC, Ericsson, Microsoft, Research In Motion, and Sony.[81] The partners divided up some 2,000 of Nortel's patents among themselves and then formed a new, independent company called Rockstar Consortium to manage the remaining 4,000 or so patents.[82]

Rockstar employs just 32 people, many of them the same people who ran Nortel's patent-licensing program. Among the employees are 10 reverse-engineering specialists whose role is to examine other companies' successful telecommunications and networking products to determine if they infringe any of the former Nortel patents. Should evidence of infringement be revealed, it is documented, and the firm contacts the infringing manufacturer seeking licensing fees for the patent(s) in question. Should the manufacturer refuse to pay the licensing fees, they could be dragged into a costly patent infringement lawsuit.[83]

Legal fees and court-awarded damages can run into the millions of dollars when companies go to court to battle over patent rights. For example, in 2007, a jury ruled Microsoft had violated patents for MP3 technology belonging to telecommunications equipment manufacturer Alcatel-Lucent. The jury awarded Alcatel-Lucent damages of $1.5 billion. Unlike large companies such as Microsoft, small companies often simply cannot afford to defend themselves against costly patent lawsuits—whether the claim is raised for legitimate reasons or as a threat against entering a new market or offering a new product. As a result, the current patent system can stifle small innovators rather than help them. Even large companies may agree to pay licensing fees rather than fight a patent infringement lawsuit.[84]

A company such as Rockstar that makes no products and whose mission is to sue or coerce manufacturers who infringe on its patents (often referred to as a pure patent operation) can become very aggressive in filing patent infringement lawsuits because it produces no products that could form the basis for a patent infringement countersuit.[85]

Prior to the sale of the Nortel patents, the Department of Justice's Antitrust Division reviewed the potential sale. There were concerns about the potential use of Nortel's standard essential patents (SEPs) as a means to slow the innovation of other companies in the telecommunications and networking industry. As a result of this review, the Department of Justice stated that its concerns were "lessened by the clear commitments by Apple and Microsoft to license SEPs on fair, reasonable, and non-discriminatory terms."[86] However, John Veschi, chief intellectual property officer at Nortel and now the CEO of Rockstar Consortium, states that Rockstar

is not bound by the promises that its member companies made. According to Veschi, "We are separate. That does not apply to us."[87]

Discussion Questions

1. Clearly state three business reasons to justify why these major IT firms formed Rockstar Consortium.
2. Although Rockstar is set up as an organization independent of its founders, what are the possible reactions if the firm aggressively pursues an important customer or supplier of one its founding companies? How might the customer or supplier react? How might the founder react?
3. Do research to determine the current status of the Rockstar Consortium. Has it been successful? Has it stirred up any further controversy?

3. Google Book Search Library Project

In 2005, Google announced the Google Book Search Library Project, a highly ambitious plan to scan and digitize books from various libraries, including the New York Public Library and the libraries at Harvard University, Oxford University, Stanford University, and the University of Michigan.[88] Google's goal is to "work with publishers and libraries to create a comprehensive, searchable, virtual card catalog of all books in all languages that helps users discover new books and publishers discover new readers."[89]

Because many of the books are protected under copyright law, Google needed a way to avoid problems with copyright infringement. Therefore, Google established a process requiring publishers and copyright holders to opt out of the program if they did not want their books to be searchable. Publishers and copyright holders were incensed and argued that they should control who can view and search their books. In October 2005, the Authors Guild and the Association of American Publishers (on behalf of McGraw-Hill, Simon & Schuster, John Wiley & Sons, Pearson Education, and the Penguin Group) filed suit against Google to stop the program. They argued that making a full copy of a copyright-protected book does not fit into the narrow exception to the law defined by fair use.

After more than two years of discussions, the parties negotiated a settlement in October 2008. The settlement did not resolve the legal dispute over whether Google's project is permissible as a fair use; however, it concluded the litigation, enabling the parties to avoid the cost and risk of a trial.[90] The proposed settlement would give Google the right to display up to 20 percent of a book online and to profit from it by selling access to all or part of it. Google would also sell subscriptions to its entire collection to universities and other institutions, but offer free portals to public libraries where users could pay a per-page fee to print parts of the book.[91] In addition, Google would set aside $125 million to compensate authors and publishers for originally infringing on their copyrights, to pay the legal fees of the authors and publishers, and to establish a Book Rights Registry where rights holders can register their works to receive a share of ad revenue and digital book sales.[92]

Google, as well as many authors and publishers, defended the settlement, saying the project would benefit authors, publishers, and the public and renew access to millions of out-of-print books.[93]

However, in a further complication, the U.S. Department of Justice (DOJ) began an inquiry in April 2009 into the proposed settlement. In September, the DOJ urged the court to reject the settlement. The DOJ concluded that the settlement violated copyright, antitrust, and class action laws on three grounds. First, one goal of the settlement was to offer copyrighted materials to the public electronically while compensating copyright holders. However, the DOJ concluded that Google's system did not require copyright owners to register. Moreover, the project includes many "orphan books"—those whose copyright holders are unknown or cannot be located. In addition, the DOJ argued that the settlement should result in a marketplace in which consumers have a choice of outlets from which they can obtain the access and in which prices are kept competitive. Finally, the DOJ harshly criticized the settlement because, as a class action, it failed to protect the rights of absent class members. The DOJ generally questioned whether a class action lawsuit was an appropriate method of dealing with the issues that arise from such a large-scale project to provide public electronic access to copyrighted material. A more appropriate venue, the DOJ suggested, would be the legislature.[94]

The parties in the case quickly responded by working out a new agreement. Through the revised agreement, Google's book registry would actively seek out authors and rights holders and Google would only scan books in English-speaking countries. In addition, the settlement limited ways that Google could make money from the project.[95]

In February 2010, however, the DOJ rejected the amended settlement for violating class action, antitrust, and copyright laws. The DOJ made specific suggestions to help avoid copyright infringement, such as arranging for authors to opt in rather than opt out and listing a book in the registry for two years prior to making it available online. But, from an antitrust perspective, the arrangement was still extremely problematic, the DOJ noted, as there are no serious competitors in the market. Amazon has approximately three million to Google's tens of millions of books.[96]

This time the parties did not rush to develop a new agreement. Instead, New York Federal District Judge Denny Chin postponed a ruling on the agreement a few weeks later.[97] The judge wanted to give all parties involved time to submit comments on the amended agreement.[98] The court issued no ruling during 2010. Then in December 2010, Google launched its own online bookstore of eBooks. Of its over three million titles, only 200,000 had been licensed through publishers. The remaining 2.8 million were texts no longer covered by copyright law in the United States.[99]

Discussion Questions

1. Do you think that Google should have taken a different approach that would have allowed it to avoid litigation and a lengthy delay in implementing its Book Search Library Project? Please explain your answer.
2. As a potential user, are you in favor of or do you oppose the Book Search Library Project? Please explain your answer.
3. Do you think that the proposed settlement gives Google an unfair advantage to profit from creating an online service that allows people to access and search millions of books?

End Notes

[1] Michael Riley and Ashlee Vance, "Inside the Chinese Boom in Corporate Espionage," *Bloomberg Businessweek*, March 15, 2012, www.businessweek.com/articles/2012-03-14/inside-the-chinese-boom-in-corporate-espionage.

[2] Allan Chernoff, "Could the Lights Go Out in the Northeast?" *CNN*, July 9, 2010, www.cnn.com/video/#/video/us/2010/07/09/chernoff.northeast.power.threat.cnn.

[3] AMSC, "About Us," www.amsc.com/about/index.html (accessed February 16, 2013).

[4] Michael Riley and Ashlee Vance, "Inside the Chinese Boom in Corporate Espionage," *Bloomberg Businessweek*, March 15, 2012, www.businessweek.com/articles/2012-03-14/inside-the-chinese-boom-in-corporate-espionage.

[5] Michael Riley and Ashlee Vance, "Inside the Chinese Boom in Corporate Espionage," *Bloomberg Businessweek*, March 15, 2012, www.businessweek.com/articles/2012-03-14/inside-the-chinese-boom-in-corporate-espionage.

[6] Keith Johnson, "China Court to Weigh Corporate-Spy Case," *Wall Street Journal*, October 25, 2012, http://online.wsj.com/article/SB10001424052970203937004578078603748811898.html.

[7] Keith Johnson, "China Court to Weigh Corporate-Spy Case," *Wall Street Journal*, October 25, 2012, http://online.wsj.com/article/SB10001424052970203937004578078603748811898.html.

[8] Diarmaid Williams, "Fresh Twist in AMSC-Sinovel Legal Case," PEi Power Engineering International, January 14, 2013, www.powerengineeringint.com/articles/2013/01/Fresh-twist-in-AMSC-Sinovel-legal-case.html.

[9] Michael Riley and Ashlee Vance, "Inside the Chinese Boom in Corporate Espionage," *Bloomberg Businessweek*, March 15, 2012, www.businessweek.com/articles/2012-03-14/inside-the-chinese-boom-in-corporate-espionage.

[10] Keith Johnson, "China Court to Weigh Corporate-Spy Case," *Wall Street Journal*, October 25, 2012, http://online.wsj.com/article/SB10001424052970203937004578078603748811898.html.

[11] Matt Pilon, "AMSC Looks Ahead After Trimming Losses," Worcester Business Journal Online, February 12, 2013, www.wbjournal.com/apps/pbcs.dll/article?AID=/20130212/METROWEST01/130219991.

[12] U.S. Code, Title 17, § 102(a).

[13] "Sonny Bono Copyright Term Extension Act," *EconomicExpert.com*, www.economicexpert.com/a/Sonny:Bono:Copyright:Term:Extension:Act.htm (accessed February 15, 2013).

[14] Eldred v. Ashcroft, Legal Information Institute, www.law.cornell.edu/supct/search/display.html?terms=copyright&url=/supct/html/01-618.ZS.html (accessed February 15, 2013).

[15] Joseph C. Self, "The 'My Sweet Lord'/'He's So Fine' Plagiarism Suit," http://abbeyrd.best.vwh.net/mysweet.htm (accessed February 15, 2013).

[16] "17 USC Section 107 – Limitations on Exclusive Rights: Fair Use," www.law.cornell.edu/uscode/text/17/107 (accessed April 17, 2013).

[17] HathiTrust Digital Library, "About," www.hathitrust.org/access (accessed February 15, 2013).

[18] "The HathiTrust Case Decision: Empowering the Fair Use Doctrine," *Legal Solutions Blog*, October 22, 2012, http://westlawinsider.com/cyberlaw/the-hathitrust-case-decision-empowering-the-fair-use-doctrine.

[19] Andrew Albanese, "Google Scanning Is Fair Use Says Judge," *Publishers Weekly*, October, 11, 2012, http://publishersweekly.com/pw/by-topic/digital/copyright/article/54321-in-hathitrust-ruling-judge-says-google-scanning-is-fair-use.html.

[20] Tetris, "The History of Tetris," www.tetris.com/history/index.aspx (accessed February 16, 2013).

[21] Charles Bieneman, "Copying the Look and Feel of Tetris Is Software Copyright Infringement," *The Software Intellectual Property Report*, May 31, 2012, http://swipreport.com/copying-the-look-and-feel-of-tetris-is-software-copyright-infringement.

[22] Adrienne Kendrick, "Tetris Gets Permanent Injunction Against Xio," *IPWatchdog*, February 12, 2013, www.ipwatchdog.com/2013/02/12/tetris-gets-permanent-injunction-against-xio/id=34996.

[23] United States Department of Justice, "PRO IP Act: Annual Report FY2012," December 2012, www.justice.gov/dag/iptaskforce/proipact/doj-pro-ip-rpt2012.pdf.

[24] World Trade Organization, "What Is the WTO?," www.wto.org (accessed February 17, 2013).

[25] World Intellectual Property Organization, "What Is WIPO?," www.wipo.int/about-wipo/en/what_is_wipo.html (accessed February 17, 2013).

[26] "Viacom v. YouTube," Digital Media Law Project, www.dmlp.org/threats/viacom-v-youtube (accessed February 18, 2013).

[27] Robyn Hagan Cain, "Viacom Lawsuit Reinstated: Will DMCA Safe Harbor Save YouTube?," *U.S. Second Circuit* (blog), http://blogs.findlaw.com/second_circuit/2012/04/viacom-lawsuit-reinstated-will-dmca-safe-harbor-save-youtube.html.

[28] *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 17, 2003, www.judiciary.senate.gov/hearings/testimony.cfm?id=4f1e0899533f7680e78d03281ff07397&wit_id=4f1e0899533f7680e78d03281ff07397-0-1 (accessed February 18, 2013).

[29] IBM, "20 Years of Patent Leadership and Innovation," www.research.ibm.com/articles/patents.shtml (accessed February 21, 2013).

[30] Joff Wild, "More on the IBM $1 Billion Patent Licensing Urban Legend," *Intellectual Asset Management*, March 27, 2008, www.iam-magazine.com/blog/Detail.aspx?g=9be3f156-79b1-49f4-abf1-9bee7e788501.

[31] Microsoft Patent Ranking Slips in 2011 as IBM Retains the Crown," *Geek Wire*, January 12, 2012, www.geekwire.com/2012/microsoft-patent-ranking-slips-2011-ibm-retains-crown.

[32] The United States Patent and Trademark Office, "December 2012 Patents Data, at a Glance," Data Visualization Center (accessed March 28, 2013) www.uspto.gov/dashboards/patents/main.dashxml.

[33] 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.

[34] Nathan Hurst, "How the America Invents Act Will Change Patenting Forever," March 15, 2013, *Wired*, www.wired.com/design/?p=146445.

[35] 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.

[36] "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 February 26, 2013).

[37] *Diamond v. Diehr*, 450 U.S. 175(1981), BitLaw, www.bitlaw.com/source/cases/patent/Diamond_v_Diehr.html (accessed February 21, 2013).

[38] "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 February 26, 2013).

[39] Timothy B. Lee, "The Supreme Court Should Invalidate Software Patents," *Forbes*, July 28, 2011.

[40] Thomas Claburn, "Google Beats Oracle Patent Claim," *InformationWeek*, May 23, 2012, www.informationweek.com/software/operating-systems/google-beats-oracle-patent-claim/240000926.

[41] "The Biggest Patent Lawsuits of 2012," *TechBeat*, October 16, 2012, techbeat.com/2010/the-biggest-patent-lawsuits-of-2012.

[42] "The Biggest Patent Lawsuits of 2012," *TechBeat*, October 16, 2012, techbeat.com/2010/the-biggest-patent-lawsuits-of-2012.

[43] "The Biggest Patent Lawsuits of 2012," *TechBeat*, October 16, 2012, techbeat.com/2010/the-biggest-patent-lawsuits-of-2012.

[44] 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=feedburner&utm_medium=feed&utm_campaign=Feed%3A+androidandme+%28Android+and+Me%29&utm_content=NewsGator+Online.

[45] Invention Statistics, "Patent Litigation Costs, How Much Does It Cost to Protect a Patent?," www.inventionstatistics.com/Patent_Litigation_Costs.html (accessed February 23, 2013).

[46] "Toys R Us Sued Over Kids Tablet Trade Secrets," Reuters, September 24, 2012, www.reuters.com/article/2012/09/24/us-toysrus-tablet-lawsuit-idUSBRE88N0WM20120924.

[47] National Conference of Commissioners on Uniform State Laws, "Uniform Trade Secrets Act," http://euro.ecom.cmu.edu/program/law/08-732/TradeSecrets/utsa.pdf (accessed February 25, 2013).

[48] Gerald J. Mossinghoff, J. Derek Mason, PhD., 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.

[49] Ryan Averbeck and Gregory A. Gaddy, "Protecting Your Organization's Innovations," *CSO Online*, February 22, 2009, www.csoonline.com/article/481815/protecting-your-organization-s-innovations.

[50] DuPont, "Our Company," www2.dupont.com/corp/en-us/our-company/index.html (accessed February 25, 2013).

[51] Executive Office of the President of the United States, "Administration Strategy on Mitigating the Theft of U. S. Trade Secrets," February 2013, http://info.publicintelligence.net/WH-EconomicEspionage.pdf.

[52] Thomas Claburn, "Apple's Controversial iPhone Developer Agreement Published," *InformationWeek*, October 28, 2008, www.informationweek.com/personal-tech/smart-phones/apples-controversial-iphone-developer-ag/211601121.

[53] Bill Nolan, "Noncompete Agreements: Critical IP and Employment Protection," *Columbus CEO*, February 14, 2011, www.columbusceo.com/parting_shots/article_56dd9cf4-3884-11e0-a106-0017a4a78c22.html.

[54] Jon Newberry, "Vantiv Sues Former Exec, Wants Court to Enforce Non-Compete," *Business Courier*, December 21, 2012, www.bizjournals.com/cincinnati/news/2012/12/21/vantiv-sues-former-exec-wants-court.html.

[55] Jonathan Stempel, "Apple, Google, Intel Fail to Dismiss Staff Poaching Lawsuit," Reuters, April 19, 2012, www.reuters.com/article/2012/04/19/us-apple-poaching-lawsuit-idUSBRE83I0VF20120419.

[56] 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.

[57] 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.

[58] Turnitin, "About Turnitin," http://turnitin.com/en_us/about-us/our-company (accessed March 16, 2013).

[59] iThenticate, "About iThenticate," www.ithenticate.com/about (accessed March 16, 2013).

[60] "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 March 16, 2013).

[61] 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.

[62] Google, "Discover the World of Open Source with Google Code-in 2012," Official Google Blog, November 20, 2012, http://googleblog.blogspot.in/2012/11/discover-world-of-open-source-with.html.

[63] Omar Akhtar, "How the Biz World Took a Page from the CIA," *Fortune*, December 20, 2012.

[64] "Dorothy's Decision Matrix," *Einsight* (blog), October 6, 2010, www.scottpublicrelations.com/eblog/?s=girls+wrestling.

[65] "What Is Trademark Fair Use?," Trademark Education & Information, www.trademark-education.com/fairuse.html (accessed March 15, 2013).

[66] *Playboy Enterprises, Inc. v. Terri Welles*, www.loundy.com/CASES/Playboy_v_Wells.html (accessed March 15, 2013).

[67] Kenneth Rapoza, "Apple Closer to Solution Regarding Brazilian iPhone Trademark Dispute," *Forbes*, March 9, 2013.

[68] Ally Financial, "About Ally," www.ally.com/about/company-structure/history (accessed March 15, 2013).

[69] Steve Levy, "Ally Sues Cybersquatting Enemy," Domainnamestrategy.com (blog), January 25, 2013, www.domainnamestrategy.com/category/categories/cybersquatting.

[70] Alice Corporation, "About Us," www.alicecorp.com/fs_about_us.html (accessed March 31, 2013).

[71] "Federal Circuit Finds Business Method Patentable," Thomson Reuters, July 9, 2012, http://newsandinsight.thomsonreuters.com/Legal/News/2012/07_-_July/Federal_Circuit_finds_business_method_patentable.

[72] Jacob Sugarman, "When Patent Trolls Attack," *Salon*, February 7, 2013, www.salon.com/2013/02/07/when_patent_trolls_attack/.

[73] Timothy B. Lee, "Supreme Court Orders Do-Over on Key Software Patent Ruling," *Ars Technica*, May 23, 2012, http://arstechnica.com/tech-policy/2012/05/supreme-court-orders-do-over-on-key-software-patent-ruling.

[74] Timothy B. Lee, "Supreme Court Orders Do-Over on Key Software Patent Ruling," *Ars Technica*, May 23, 2012, http://arstechnica.com/tech-policy/2012/05/supreme-court-orders-do-over-on-key-software-patent-ruling.

[75] *State Street Bank and Trust Company v. Signature Financial Group*, Majority Decision, Senior Judge Rich, July 1998, 10, 4, 24ff. https://bulk.resource.org/courts.gov/c/F3/149/149.F3d.1368.96-1327.html#fn4_ref.

[76] David Balto, Previewing *CLS Bank v. Alice*, February 7, 2013, www.patentprogress.org/2013/02/07/previewing-cls-bank-v-alice.

[77] "Case 1:07-Cv-00974 – CLS Bank v. Alice – USA Amicus ISO Neither Party," Patent Progress, February 7, 2013, www.patentprogress.org/documents/case-107-cv-00974-cls-bank-v-alice-usa-amicus-iso-neither-party.

[78] Matthew Broersma, "Rockstar Consortium Launches Patent Attacks," *Tech Week Europe*, May 28, 2012, www.techweekeurope.co.uk/news/news-apple/rockstar-consortium-launches-patent-attacks-79901.

[79] Nortel, "About Us," www.nortel-us.com/about (accessed March 17, 2013).

[80] Nortel, "About Us," www.nortel-us.com/about (accessed March 17, 2013).

[81] Matthew Broersma, "Rockstar Consortium Launches Patent Attacks," *Tech Week Europe*, May 28, 2012, www.techweekeurope.co.uk/news/news-apple/rockstar-consortium-launches-patent-attacks-79901.

[82] Mike Masnick, "Apple and Microsoft Behind Patent Troll Armed with Thousands of Nortel Patents", *Tech Dirt*, May 23, 2012, www.techdirt.com/articles/20120521/13194719006/apple-microsoft-behind-patent-troll-armed-with-thousands-nortel-patents.shtml.

[83] Matthew Broersma, "Rockstar Consortium Launches Patent Attacks," *Tech Week Europe*, May 28, 2012, www.techweekeurope.co.uk/news/news-apple/rockstar-consortium-launches-patent-attacks-79901.

[84] Robert McMillan, "How Apple and Microsoft Armed 4,000 Patent Warheads," *Wired*, May 21, 2012, www.wired.com/wiredenterprise/2012/05/rockstar.

[85] Matthew Broersma, "Rockstar Consortium Launches Patent Attacks," *Tech Week Europe*, May 28, 2012, www.techweekeurope.co.uk/news/news-apple/rockstar-consortium-launches-patent-attacks-79901.

[86] Matthew Broersma, "Rockstar Consortium Launches Patent Attacks," *Tech Week Europe*, May 28, 2012, www.techweekeurope.co.uk/news/news-apple/rockstar-consortium-launches-patent-attacks-79901.

[87] Robert McMillian, "How Apple and Microsoft Armed 4,000 Patent Warheads," *Wired*, May 21, 2012, www.wired.com/wiredenterprise/2012/05/rockstar.

[88] Jonathan Band, "The Google Library Project: Both Sides of the Story," www.plagiary.org Google-Library-Project.pdf (accessed March 21, 2011).

[89] Google Book Search, "Google Books Library Project," http://books.google.com/google-books/library.html.

[90] Association of Research Libraries, "A Guide for the Perplexed: Libraries and the Google Library Project Settlement," November 13, 2008, www.arl.org/bm~doc/google-settlement-13nov08.pdf.

[91] Stephanie Condon, "Google Reaches $125 Million Settlement with Authors," *CNET*, October 28, 2008, http://news.cnet.com/8301-13578_3-10076948-38.html.

[92] Chris Snyder, "Google, Authors and Publishers Settle Book-Scan Suit," *Wired*, October 28, 2008, www.wired.com/epicenter/2008/10/google-authors.

[93] Miguel Helft, "Justice Dept. Opens Antitrust Inquiry into Google Books Deal," *New York Times*, April 28, 2009.

[94] "Statement of Interest of the United States Regarding Proposed Amended Settlement," *The Authors Guild, Inc. etal, Plaintiffs, v. Google Inc., Defendant;* 05 Civ. 8136 (DC) ECF Case, Filed September 18, 2009, http://thepublicindex.org/docs/letters/usa.pdf (accessed April 20, 2011).

[95] Elinor Mills, "Google Books Settlement Sets Geographic, Business Limits," *CNET*, November 13, 2009, http://news.cnet.com/8301-1023_3-10397787-93.html.

[96] "Statement of Interest of the United States Regarding Proposed Class Settlement," *The Authors Guild, Inc. et a*l., *Plaintiffs, v. Google Inc., Defendant;* 05 Civ. 8136 (DC) ECF Case, Filed February 4, 2010, http://thepublicindex.org/docs/amended_settlement/usa.pdf (accessed April 19, 2011).

[97] Motoko Rich, "Judge Hears Arguments on Google Book Settlement," *New York Times*, February 18, 2010, www.nytimes.com/2010/02/19/technology/19google.html.

[98] Greg Sandoval, "Google Book Settlement Draws Fire in Court," *CNET*, February 18, 2010, http://news.cnet.com/8301-31001_3-10456382-261.html.

[99] Ryan Singel, "Google Launches Online Bookstore, Challenging Amazon," *Wired*, December 6, 2010, www.wired.com/epicenter/2010/12/google-bookstore.

CHAPTER 7

SOFTWARE DEVELOPMENT

QUOTE

Any process that tries to reduce software development to a "no brainer" will eventually produce just that: a product developed by people without brains.

—Andy Hunt and Dave Thomas, "Cook Until Done"

VIGNETTE

Stock Markets Susceptible to Software Glitches

Regulation National Market System (Reg NMS) is a set of rules implemented by the Securities and Exchange Commission in 2007 to boost competition across the various stock exchanges. Reg NMS essentially enables traders to do comparison shopping across the various exchanges to find the best price. The rules also had the effect of lowering trading costs and accelerating the speed of trade executions to a split second.[1] The implementation of Reg NMS led to a rise in the number of firms engaged in "high-frequency trading"—that is, trading that uses powerful computers and complex computer algorithms to trade hundreds or even thousands of times a day. High-frequency trading often employs stock holding periods of only a few seconds to take advantage of tiny price changes.[2] Unfortunately, there have been several recent examples in which problems with the software used in high-frequency trading operations have wreaked havoc on the market—causing problems for the listed companies and stock traders alike.

On May 6, 2010, a "flash crash" of U.S. stock markets occurred in which the Dow Jones Industrial average dropped over 700 points in five minutes, only to recover 600 points over the course of the next 20 minutes. It was a roller coaster ride that briefly erased $1 trillion in market value and left investors and regulators struggling to understand what had happened.[3] Ultimately, it was determined that the flash crash was caused by the actions of a single, large investor who was using automated trading software to trade futures on the stocks in the Standard & Poor 500 stock index. The software placed large sell orders that were, at first, absorbed by other buyers—many of whom were also using automated trading software. However, the algorithm used by the seller's trading software responded to the increase in market activity in the futures contracts by automatically placing larger and larger sell orders, which the market could no longer absorb. This resulted in a rapid decline in the prices of the underlying stocks.[4]

Better Alternative Trading System (BATS) is the third-largest equities exchange operator in the United States. The BATS Exchange accounts for 11 percent of the trading volume of U.S. stock shares.[5,6] On March 23, 2012, the day that BATS launched its own initial public offering (IPO), a "bad trade" for shares of Apple at an incorrect price was accepted on the BATS Exchange. This triggered a flurry of high-frequency trading that resulted in a 9.4 percent drop in Apple's stock's price in just five minutes. The sudden drop in price triggered a trading "circuit breaker" that halted trading in Apple shares and likely prevented a broader crash affecting other stocks. As it turned out, BATS was having technical problems in processing orders for any companies whose ticket symbol was in the range of A to BF, a range that includes not only Apple, but also the firm's own symbol BATS. The BATS stock opened at $16 per share, and at one point appeared to be selling at less than a penny per share. Eventually BATS was forced to halt trading of its own stock and cancel all trades of the stock for that day. BATS also pulled its IPO, which was put on hold "for the foreseeable future."[7,8]

In May 2012, computer problems on the NASDAQ stock exchange disrupted Facebook's IPO. As a result, Facebook trading was delayed half an hour beyond the normal trading time for an IPO. Once trading began, over 80 million shares of Facebook were traded in the first 30 seconds, but traders complained that their orders were not being completed promptly and that they were being charged more than expected. Traders also complained that they were not getting confirmation on their Facebook trades; thus, they did not know if they owned the stock or not.

Knight Capital is a global financial services firm that engages in market making of U.S. securities and electronic stock transaction execution. As a market maker, the firm holds a large quantity of shares of various stocks to facilitate trading in those stocks. The firm displays buy and sell prices it is willing to accept and when an order is received, the market maker immediately fills a buy order from its own inventory or finds a buyer for a sell order. All this happens in seconds. In August 2012, following the installation of new trading software, Knight Capital's computers sent incorrect orders for over 140 stocks listed on the New York Stock Exchange.[9] As a result, several of these stocks traded at 20 times their normal volume and lost over 10 percent of their value in a matter of seconds before recovering.[10] After sorting through the transactions, the New York Stock Exchange canceled trades in the stocks that were most affected by the problem. In the days following the glitch, Knight Capital's own stock price fell from just over $10 per share to under $3 per share.[11]

According to the rules of the stock exchanges, stock orders must be routed to those exchanges that offer the best bid and offer prices. In January 2013, BATS was forced to acknowledge more software-related problems when it notified its clients that due to problems with its trading software, the firm did not meet that requirement for many orders. As a result, over the course of four years, hundreds of thousands of orders were executed at inferior prices.[12] The full fallout from this admission is yet to be seen, but trader lawsuits and other repercussions can be expected.

Questions to Consider

1. Do you think that the software development teams responsible for the development of programs to support high-frequency trading and other sophisticated trading tools should bear any responsibility for these trading fiascos? Why or why not?
2. What measures could be taken to improve the quality of trading software to avoid the problems discussed in the opening vignette?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. Why must companies place an increased emphasis on the use of high-quality software in business systems, industrial process-control systems, and consumer products?
2. What potential ethical issues do software manufacturers face in making trade-offs between project schedules, project costs, and software quality?
3. What are the four most common types of software product liability claims?
4. What are the essential components of a software development methodology, and what are the benefits of using such a methodology?
5. How can the Capability Maturity Model Integration® improve an organization's software development process?
6. What is a safety-critical system, and what special actions are required during its development?

STRATEGIES FOR ENGINEERING QUALITY SOFTWARE

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. Now that computers and software have become integral parts of almost every business, 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 Web sites. 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 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 notable software bugs that have occurred recently:

- Nokia's Lumina 900 smartphone had a software problem that could cause the device to lose its high-speed data connection. The company had hoped that the new smartphone would help raise its share of the U.S. market, which had slipped below 1 percent. The software glitch was a major setback for the firm and caused it to lower its profit forecasts. As a result, Nokia shares hit a 15-year low.[13]
- The IRS plans to invest $1.3 billion through 2024 to update its software for handling the filing of tax returns; however, an early change designed to speed up the processing of tax returns resulted in refunds that were delayed by up to 10 days for millions of taxpayers in 2012.[14]
- Some 4,000 owners of the 2013 Chevy Volt were informed that a software bug could cause their plug-in hybrid car's electric motor to shut down while the vehicle is in motion.[15]
- In late 2012, many people looking to take part in a Georgia Powerball game were upset when a software error interrupted sales of tickets for the $425 million jackpot. The problem was widespread, affecting many locations in Georgia, lasting most of the day of the drawing.[16]
- Washington State University recently implemented a $15 million software system designed to handle all major student processes—from registering for class, to paying tuition, to scheduling of advisers. Unfortunately, user unfamiliarity with the system and software bugs led to lengthy delays in processing financial aid. Many students who normally rely on financial aid had to dip into reserve funds or call upon parents to help pay for tuition, books, housing, and food until they could receive their financial aid.[17]

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 **deliverables**. 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.

A primary cause of poor software quality is that many developers do not know how to design quality into software from the very start; some 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. According to one study, even experienced software developers unknowingly inject an average of one design or implementation defect for every 7 to 10 lines of code. The developers aren't incompetent or lazy—they're just human. Everyone makes mistakes, but in software, these mistakes can result in defects.

Based on an analysis of a sample of 300 million lines of commercial code, Coverity (a software development testing firm) found that the average number of defects per thousand lines of code developed by software manufacturing companies was .64.[18] The Microsoft Windows 7 operating system contains more than 50 million lines of code. Assuming the Microsoft software developers produced code at this accuracy rate, there would still be roughly 32,000 defects in Windows 7. Thus, critical software used daily by workers worldwide likely contains tens of thousands of defects. Interestingly, based on an analysis of 37 million lines of open source code, Coverity found that the average number of defects per thousand lines of code was .45 or 30% less than in commercial code.[19]

Another factor that can contribute to poor-quality software is the extreme pressure that software companies feel to reduce the time to market for 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. 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 they expend to ensure that their products and services meet customers' expectations?" Over 1.25 million apps have been created for the various types of mobile devices; however, it is estimated that less than 20 percent of these apps exceed 1,000 downloads because of faulty software quality that results in poor application performance.[20] 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. Thus, customers challenge whether to cut software quality in favor of feature enhancement.

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 operating conditions change. For instance, software in the Cincinnati Bell telephone switch had been thoroughly tested and had operated successfully for months

after it was deployed. However, when the time changed from daylight saving time to standard time for the first time after the software was deployed, the switch failed because it was overwhelmed by the number of calls to the local "official time" phone number from people who wanted to set their clocks. The large increase in the number of simultaneous calls to the same number was a change in operating conditions that no one had anticipated.

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 include 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, radios, stereos, 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 software can put it ahead of or behind its competitors. Software problems may have caused frustrations in the past, but mismanaged software can now 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 use of software introduces product liability issues that concern many executives.

SOFTWARE PRODUCT LIABILITY

Software product litigation is certainly not new. One lawsuit in the early 1990s involved a financial institution that became insolvent because defects in a purchased software application caused errors in its integrated general ledger system, customers' passbooks, and loan statements. Dissatisfied depositors responded by withdrawing more than $5 million. Another case involved an accident that occurred when a Ford truck stalled because of a software defect in the truck's fuel injector. In the ensuing accident, a young child was killed.[21] A state supreme court later affirmed an award of $7.5 million in punitive damages against the manufacturer. In 2008, a faulty onboard computer caused a Qantas passenger flight traveling between Perth and Singapore to plunge some 8,000 feet in 10 seconds, injuring 46 passengers. Qantas moved quickly to compensate all passengers with a refund of their ticket prices, a $2,000 travel voucher, and a promise to pay all medical-related expenses. Even so, the Australian law firm of Slater & Gordon was engaged to represent a dozen of the passengers.[22]

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. Software product liability claims are typically based on strict liability, negligence, breach of warranty, or misrepresentation—sometimes in combination with one another.

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.

As discussed in Chapter 2, 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 or 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 may be warranted to run on a given machine configuration, often no assurance is given as to what that software will do. 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 a warranty disclaimer is 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 the supplier did not fulfill 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 new 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.[23] Even if breach of warranty can be proven, the damages are generally limited to the amount of money paid for the product.

As mentioned in Chapter 2, 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.

Software Development Process

Developing information system software is not a simple process; it requires completing many complex activities, with many dependencies among the various activities. Systems analysts, programmers, 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 and has 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 **software development methodology**—a standard, proven work process that enables systems analysts, programmers, project managers, and others to make controlled and orderly progress while developing high-quality software. A methodology defines activities in the software development process and the individual and group responsibilities for accomplishing these activities. It also 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. See Figure 7-1. If an organization has developed such a methodology, it is typically applied to any software development that the company undertakes.

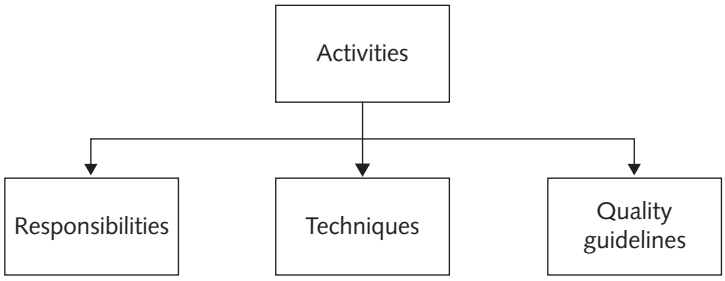


FIGURE 7-1 Software development methodology
Source Line: Course Technology/Cengage Learning.

As with most things, it is usually easier and cheaper to avoid software problems from the beginning, rather than 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 (requirements definition) can be up to 100 times less than removing a defect in a piece of software that has been distributed to customers (see Figure 7-2).[24,25] Although these studies were conducted several years ago, their results still hold true today.

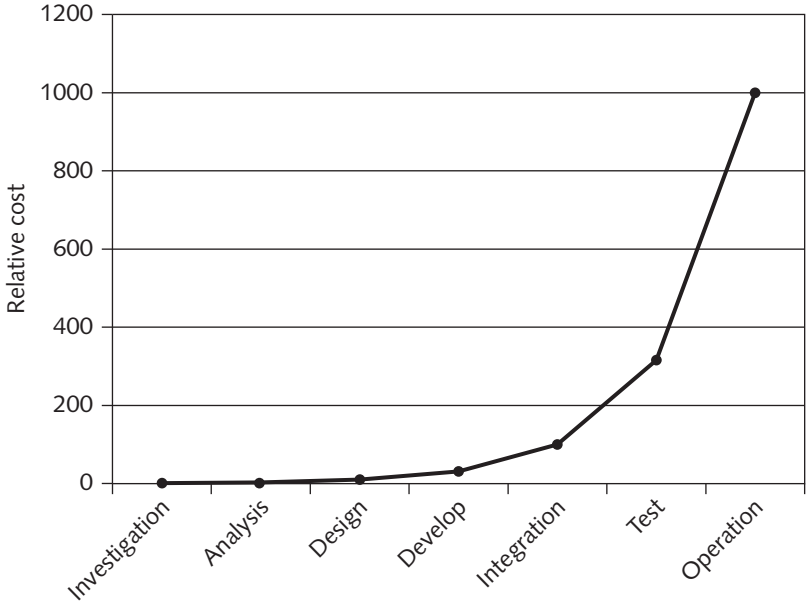


FIGURE 7-2 The cost of removing software defects
Source Line: Used with permission from LKP Consulting Group.

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 be serious in terms of liability exposure.

Quality assurance (QA) refers to methods within the development cycle 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 ships to ensure some degree of quality.

Several types of tests are used in software development, as discussed in the following sections.

Dynamic 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 with 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 Types of Software Testing

Other forms of software testing include the following:

- *Static testing*—Special software programs called static analyzers are run against new code. Rather than reviewing input and output, the static analyzer looks for suspicious patterns in programs that might indicate a defect.
- *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*—Independent testing is performed by trained end users to ensure that the system operates as they expect.

Capability Maturity Model Integration

Capability Maturity Model Integration (CMMI)—developed by the Software Engineering Institute at Carnegie Mellon—is a process-improvement approach that defines the essential elements of effective processes. The model is 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. CMMI defines five levels of software development maturity (see Table 7-1) and identifies the issues that are most critical to software quality and process improvement.

TABLE 7-1 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 Line: Used with permission from Carnegie Mellon University.

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.

Table 7-2 shows the percentages of organizations at each CMMI maturity level, as reported in a recent survey of 5,159 reporting organizations as of September 2012.

TABLE 7-2 Maturity level distribution across a large sample of organizations

Maturity level	Percent of 5,159 organizations surveyed
Not provided	3.3%
Initial	0.8%
Managed	22.1%
Defined	66.8%
Quantitatively managed	1.6%
Optimizing	6.5%

Source Line: Used with permission from Carnegie Mellon University.

The Software Engineering Institute documented the following results from CMMI process-improvement implementations at 11 different organizations:

- A 33 percent decrease in the cost to fix defects
- A 20 percent reduction in unit software costs
- A 30 percent increase in productivity
- An increase in project-schedule milestones met—from 50 percent to 95 percent[26]

CMMI-DEV is a set of guidelines for 22 process areas related 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.

At the Rolling Meadows campus of Northrop Grumman, workers design, develop, and manufacture advanced electronic systems for customers worldwide. The campus was recently assessed and rated at CMMI Level 5. According to Dan Blase, director of engineering at the facility, "Continuous improvement is an integral part of the culture at Northrop Grumman. This CMMI rating reflects our commitment to performing at the highest level for our customers, and doing so in the most affordable manner possible."[27]

KEY ISSUES IN SOFTWARE DEVELOPMENT

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 such factors as cost, ease of use, and time to market require extremely serious examination. The next sections discuss safety-critical systems and the special precautions companies must take in developing them.

Development of Safety-Critical Systems

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 automobiles' antilock brakes, nuclear power plant reactors, airplane navigation, elevators, and numerous medical devices, to name just a few. 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 lead[s] to disastrous consequences."[28] 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. Here are several examples of safety-critical system failures:

- The *Mariner I* space probe, which was intended to make a close flyby of the planet Venus, was ordered destroyed less than five minutes after launch in July 1962. Faulty software code caused the flight control computer to perform a series of unnecessary course corrections, which threw the spacecraft dangerously off course.[29]
- A Royal Air Force helicopter took off from Northern Ireland in June 1994 with 25 British intelligence officials who were heading to a security conference in Inverness. Just 18 minutes into its flight, the helicopter crashed on the peninsula of Kintyre in Argyll, Scotland, killing everyone on board. The engine management software, which controlled the acceleration and deceleration of the engines, was suspected of causing the crash.[30]
- Between November 2000 and March 2002, therapy planning software at the National Oncology Institute in Panama City, Panama, miscalculated the proper dosage of radiation for patients undergoing therapy; at least eight patients died while another 20 received overdoses that caused significant health problems.[31]

- Three accidents occurred on the Big Thunder Mountain Railroad roller coaster at Disneyland between September 2003 and July 2004. One person was killed and 10 others were injured in the September accident. The California Division of Occupational Safety and Health blamed the accidents on improper maintenance, poorly trained operators, and a glitch in the ride's computer system.[32]
- In April 2007, fire broke out on a Washington, D.C., six-car Metro train as it pulled out of the L'Enfant Plaza station. Fire and smoke were seen underneath the last car, but thankfully, the flames did not penetrate the floor of the car. The train operator stopped and evacuated the passengers. It was eventually determined that the train's brake resistor grid, which checks various subsystems and voltages, overheated and caught fire. Monitoring software failed to perform as expected in detecting and preventing excess power usage in equipment on the passenger rail cars, resulting in overheating and fire.[33]

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 requirements 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 must 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.

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** is the probability of an undesirable event occurring times the probability that the event would go undetected times the magnitude of the event's consequences if it does happen. These consequences include damage to property, loss of money, injury to people, and death.

For example, if an undesirable event has a 1 percent probability of occurring, a 25 percent chance of going undetected, and a potential cost of $1,000,000, then the risk can be calculated as $0.01 \times .25 \times \$1{,}000{,}000$, or $2,500. The risk for this event would be considered greater than that of an event with a 10 percent probability of occurring, a 20 percent chance of going undetected, and a potential cost of $100 ($0.10 \times .20 \times \$100 = \$2.00$). Risk analysis is important for safety-critical systems but is useful for other kinds of software development as well.

Another key element of safety-critical systems is **redundancy**, 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 system used in IT 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 and a new one inserted in its place. Because the data has also been stored elsewhere, data on the failed disk can be rebuilt automatically without the server ever having to be shut down.

During times of widespread disaster, lack of sufficient redundant systems can lead to major problems. For example, the designers of the reactors at Japan's Fukushima Daiichi Nuclear Power Plant anticipated that a strong earthquake and even a tsunami might hit the facility. So in addition to a main power supply, backup generators were put in place to ensure that coolant could be circulated to the nuclear reactors even if the main power supply was knocked out. When a 9.0 earthquake hit the area in early 2011, it knocked out the main power supply, but the backup power supply was still working until it was hit with a tsunami 10 meters high, twice the height of what had been anticipated in the design of the redundant power supplies of the plant.[34]

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). The different versions of the software are run in parallel, and if the outputs of the different software vary, a "voting algorithm" is executed to determine which result to use. For example, if two software versions calculate the answer to be 2.4 and the third version calculates 4.1, the algorithm might choose 2.4 as the correct answer. Each software version is built by different teams of people using different approaches to write programming instructions designed to meet the users' 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 the versions should yield a correct result. Triple-version programming is common in airplane and spacecraft control systems.

After an organization determines all pertinent risks to a system, it must decide what level of risk is acceptable. This decision is extremely difficult and controversial because it involves forming personal judgments about the value of human life, assessing potential liability in case of an accident, evaluating the surrounding natural environment, and estimating the system's costs and benefits. System modifications must be made if the level of risk in the design is judged to be too great. Modifications can include adding redundant components or using safety shutdown systems, containment vessels, protective walls, or escape systems. Another approach is to mitigate the consequences of failure by devising emergency procedures and evacuation plans. In all cases, organizations must ask how safe is safe enough if human life is at stake.

Manufacturers of safety-critical systems must sometimes decide whether to recall a product when data indicates 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 had to make similar decisions, which can be complicated if data cannot pinpoint the cause of a particular problem. For example, there was great controversy in 2000 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 one chance in a thousand 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 the goal of designing a system with "five nines" (99.999%) reliability. This translates to a system that would have only 5.26 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 considerable 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 difficult 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.[35]

Quality Management Standards

The International Organization for Standardization (ISO), founded in 1947, is a worldwide federation of national standards bodies from 161 countries. The organization 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 9001:2008 provides a set of standardized requirements for a quality management system. It is the only standard in the ISO 9001 family for which organizations can be certified. Over 1 million organizations in more than 175 countries have ISO 9001 certification.[36] Although companies can use the standard 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 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 (FMEA) is an important technique used to develop ISO 9001-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.[37]

Raytheon is a technology company that designs and manufactures aerospace and defense systems that incorporate the latest electronic components. It employs 68,000 people worldwide and generated $24 billion in recent sales.[38] Raytheon employs FMEA throughout its product development life cycle. Starting early in the design cycle, the firm 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. The firm then uses this input to prioritize the product design issues that need to be eliminated or mitigated to create superior products.[39]

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

Source Line: Course Technology/Cengage Learning.

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?		

Source Line: Course Technology/Cengage Learning.

Summary

- High-quality software systems are easy to learn and use. Such systems 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, among others.
- Now that computers and software have become integral parts of almost every business, 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 Web sites.
- 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.
- 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.
- Software product liability claims are typically based on strict liability, negligence, breach of warranty, or misrepresentation—sometimes in combination.
- A software development methodology defines the activities in the software development process, defines individual and group responsibilities for accomplishing objectives, recommends specific techniques for accomplishing the objectives, and offers guidelines for managing the quality of the products during the various stages of the development cycle.
- 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: (1) by reducing the number of software errors that could cause damage and (2) 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 cycle designed to guarantee reliable operation of a product. Ideally, these methods are applied at each stage of the development cycle.
- Capability Maturity Model Integration (CMMI)—developed by the Software Engineering Institute at Carnegie Mellon—is a process-improvement approach that defines the

essential elements of effective processes. 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.
- 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 9001:2008 standard serves as a guide to quality products, services, and management. Approximately 1 million organizations in more than 175 countries have ISO 9001 certification. 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

black-box testing
breach of warranty
business information system
Capability Maturity Model Integration (CMMI)
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 system
integration testing
ISO 9001 family of standards
N-version programming
product liability
quality assurance (QA)
quality management
redundancy
reliability
risk
safety-critical system
software defect
software development methodology
software quality

static testing
strict liability
system safety engineer
system testing
user acceptance testing
warranty
white-box testing

Self-Assessment Questions

The answers to the Self-Assessment Questions can be found in Appendix B.

1. Which of the following is true about a high-quality software system?
   a. It is more difficult to learn and use.
   b. It meets its users' needs.
   c. It operates more slowly and deliberately.
   d. It operates in an unreliable manner.
2. Software _____ is the degree to which a software product meets the needs of its users.
3. Which of the following is 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. Programmers make mistakes in turning design specifications into lines of code.
   c. Software developers are under extreme pressure to reduce the time to market of their products.
   d. All of the above are major causes of poor software quality.
4. A decision support system might be used to do which of the following?
   a. process large numbers of business transactions
   b. assist managers in developing accurate forecasts
   c. control manufacturing processes
   d. perform all of the above
5. The liability of manufacturers, sellers, lessors, and others for injuries caused by defective products is commonly referred to as _____.
6. A standard, proven work process for the development of high-quality software is called a(n) _____.
7. The cost to identify and remove a defect in an early stage of software development is typically about the same as 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 software _____ is any error that if not removed could cause a software system to fail to meet its users' needs.
9. Methods within the development cycle designed to guarantee reliable operation of the product are known as _____.

10. Which of the following is a form of software testing that involves viewing a software unit as a device that has expected input and output behaviors but whose internal workings are known?
    a. dynamic testing
    b. white-box testing
    c. integration testing
    d. black-box testing
11. Which of the following is an approach that defines the essential elements of an effective process and outlines a system for continuously improving software development?
    a. CMMI-DEV
    b. FMEA
    c. ISO-9000
    d. DOD-178B
12. One of the most important and difficult areas of safety-critical system design is the system-human interface. True or False?
13. The provision of multiple interchangeable components to perform a single function to cope with failures and errors is called:
    a. risk
    b. redundancy
    c. reliability
    d. availability
14. A reliability evaluation technique that can determine the effect of system and equipment failures is _____.
15. When discussing system performance, the terms reliability and safety mean the same. True or False?
16. In a lawsuit alleging _____, responsibility is limited to harmful defects that could have been detected and corrected through "reasonable" software development practices.

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. Briefly describe and give an example of a business information system, a decision support system, and a control system.
3. Define and briefly discuss the difference between white box testing and black box testing.
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 customers. What are the implications for a software development organization?

5. Explain the difference between strict liability and negligence.
6. Identify and briefly discuss two ways that 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 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 but difficult areas of safety-critical systems? Do a search on the Internet and find three good sources of information relating to how to design an effective system-human interface.
9. What is the difference between system reliability and system safety? Give an example of a system that operates reliably but not safely.
10. Identify and briefly discuss the implications to a project team of classifying a piece of software as safety critical.
11. Your organization develops accounting software for use by individuals to budget and forecast their expenses and pay their bills while keeping track of the amount of money in their savings and checking accounts. Develop a strong argument for the management of your firm as to why the firm must conduct an assessment of its current software development practices.
12. Discuss why an organization might elect to use a separate, independent team for quality testing rather than the group of people who originally developed the software.

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 Web site 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 5 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 do?
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 developed a spreadsheet program that helps you perform your role of inventory control manager at a small retail sports shoe store. The software uses historical sales data to calculate expected weekly sales for each of about 250 shoes carried by the store. Based on that forecast, you order the appropriate shoes from the various manufacturers. Your store is one of four shoe stores owned by the same person. You sent a copy of the spreadsheet to each of the people responsible for inventory control at the other three retail stores, and they are all now using your software to help them do their jobs. You have started getting complaints that the software is not entirely accurate, and you notice that your own estimates are no longer as accurate as they used to be. What would you do?
6. 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 flying and spray caustic liquid in all directions.

   Your manager points out that the stainless steel vat is surrounded by two sets of protective concrete walls and that the reactor's human operators can intervene in case of a software failure. He feels that these measures would 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?

7. You are a senior software development consultant with a major consulting firm. You have been asked to conduct a follow-up assessment of the software development process for ABCXYZ Corporation, a company for which you had performed an initial assessment using CMMI two years prior. At the initial assessment, you determined the company's level of maturity to be level 2. Since that assessment, the organization has spent a lot of time and effort following your recommendations to raise its level of process maturity. The organization appointed a senior member of its IT staff to be a process management guru and paid him $150,000 per year to lead the improvement effort. This senior member adopted a methodology for standard software development and required all project managers to go through a one-week training course at a total cost of more than $2 million.

   Unfortunately, these efforts did not significantly improve process maturity because senior management failed to hold project managers accountable for actually using the standard development methodology in their projects. Too many project managers convinced senior management that the new methodology was not necessary for their particular project and would just slow things down. You are concerned that when senior management learns that no real progress has been made, they will refuse to accept partial blame for the failure and instead drop all attempts at further improvement. You are also likely to lose your contract with the firm. What would you do?

8. 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 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 just two 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 a viable 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. InterSystems Earns ISO 9001-2008 Certification

InterSystems is a privately held software development firm with recent sales revenue of $446 million. The company is headquartered in Cambridge, Massachusetts, with offices in 25 countries worldwide.[40] Recently, InterSystems became ISO 9001:2008 certified for all

processes related to product and service creation in connection with two of its primary products: Caché and Ensemble.[41] By meeting these requirements, InterSystems has proven that it has in place systems and processes necessary to ensure that its products and services are delivered in a controlled and repeatable manner. ISO 9001-2008 certification is proof of an organization's commitment to quality management and continuous improvement.

The Caché product is a high-performance/high-reliability database management system. The software comes bundled with an application development environment that assists programmers in the rapid development of software applications. Caché is used extensively by organizations in clinical healthcare applications to develop systems that capture, organize, and analyze healthcare records in ways that lead to better patient experiences and improved healthcare outcomes.[42]

The Johns Hopkins Cancer Center, nationally recognized as one of the leading cancer centers in the United States, is a major InterSystems customer. The hospital implemented an advanced, multifunctional oncology clinical information system based on Caché. The system records all interactions among patients, caregivers, providers, and administrators from the time they register to enter the facility until they leave and are billed. During a typical visit to the center, patients have multiple appointments with various care providers and undergo various tests and treatments. Patients are issued a bar-coded ID that is scanned at strategic locations as they move through the hospital—allowing personnel to track what appointments remain and where the patient is at any time. Key data associated with all tests, treatments, and patient results is captured so that care providers can review treatment approaches used in the past to help decide the best treatment process for new patients.[43]

Discussion Questions

1. A mission-critical system is one whose failure will result in an organization being unable to continue business operations. A safety-critical system is one whose failure will result in human injury or loss of life. Is the John Hopkins system described above mission critical or safety critical? Why? Can you give an example of a safety-critical system that is not mission critical?
2. Caché and its associated application tools constitute a system that is used to build a wide variety of information systems for customers around the world. Do you think that the Caché software and tools should be considered a safety-critical system and undergo the rigorous development process associated with such systems? If so, what would be the implications for InterSystems and its customers in terms of costs and frequency of software modifications and updates? Would this put InterSystems at a competitive disadvantage to other software development companies?
3. Should every organization that builds safety-critical systems be required to have all its system development processes and tools ISO-9000: 2008 certified? Why or why not?

2. Apple Guidelines for App Approval

Apple's App Store has been a huge success ever since it was launched in 2008. As of April 2013, the App Store offered more than 500,000 applications available for sale to owners of Apple iPhone, iPad, and iPod devices—with more than 4 billion downloads in the first quarter of 2013.[44]

Before software applications can be sold through the App Store, they must go through a review process. Apple has been accused by some of using clandestine and capricious rules to reject some programs—thus, blocking them from reaching the very large and growing market of iPhone, iPad, and iPod Touch users. One application developer complained: "If you submit an app, you have no idea what's going to happen. You have no idea when it's going to be approved or if it's going to be approved."[45] The developers of an app called "South Park" complained that their app was rejected because the content was deemed "potentially offensive," even though episodes of the award-winning animated sitcom are available at the Apple iTunes Store.[46] In September 2010, after more than two years of complaints, Apple finally provided application developers the guidelines it uses to review software.

Most guidelines seem to be aimed at ensuring that Apple users can only access high-quality and noncontroversial apps from its App Store. Some of the Apple guidelines are clear and their rationale is easy to understand, such as "apps that rapidly drain the device's battery or generate excessive heat will be rejected." However, other guidelines are unclear and highly subjective, such as "We will reject apps for any content or behavior that we believe is over the line. What line, you ask? Well, as a Supreme Court Justice once said, 'I'll know it when I see it.' And we think that you will also know it when you cross it."[47] ("I know it when I see it" was the phrase used by U.S. Supreme Court Justice Potter Stewart to describe his ability to recognize rather than to provide a precise definition of hard core pornography in his opinion in the case *Jacobellis v. Ohio* in 1964.)

The Electronic Frontier Foundation believes that while the guidelines are helpful, in some cases Apple is defining the content of third-party software and placing limits on what is available to customers of Apple's App Store.[48]

By way of comparison, Google places few restrictions on developers of software for its competing Android Marketplace. However, there have been many low-quality applications offered to Android Marketplace customers, including some that include malware. Indeed by early 2011, Google had pulled 21 Android applications from its Android Marketplace because, once downloaded, the applications not only stole users' information and device data, but also created a backdoor for even more harmful attacks.[49] Apple's decision to finally share its applications guidelines may have been an attempt to combat the rapidly increasing popularity of the Android.[50] It may also have been a response to a U.S. Federal Trade Commission investigation of a complaint from Adobe concerning Apple's banning of the Flash software from devices that run Apple's iOS operating system. (Adobe® Flash® Player is a browser-based application that runs on many computer hardware/operating system combinations and supports the viewing of so called "rich, expressive applications," content, and videos across screens and browsers.)[51]

Discussion Questions

1. Should Apple conduct extensive screening of apps before they are allowed to be sold on the App Store? Why or why not?
2. Do research to determine the current status of the FCC investigation of Apple for banning use of the Adobe Flash software on devices that use the iOS operating system.
3. What do you think of Apple's guideline that says it will reject an app for any content or behavior that they believe is "over the line"? Could such a statement be construed as a violation of the developer's freedom of speech? Why or why not?

3. Software Errors Lead to Death

Medical linear accelerators have long been a critical piece of medical equipment in the fight against cancer. Linear accelerators deliver radiation therapy to cancer patients by accelerating electrons to create high-energy beams, which can kill cancer tumors without impacting surrounding healthy tissue. Tumors close to the skin can be treated with the accelerated electrons; however, for tumors that are more deeply embedded, the electron beam is converted into an X-ray photon beam, which is diffused using a beam spreader plate.

The Canadian firm Atomic Energy of Canada Limited (AECL) and a French company named CGR collaborated to build two models of medical linear accelerators. One model, the Therac-6, was capable of producing only X-rays that could be used to kill tumors close to the skin. A later model, the Therac-20, was capable of producing both X-ray photons and electrons and thus could kill both shallow and deeply embedded tumors. Computer software was used to simplify the operation of the equipment but not to control and monitor its operation. Instead, industry standard hardware safety features were built into both models.[52]

After the business relationship between the two firms failed, AECL went on to build the Therac-25 based on a new design concept. Unlike the Therac-6 and Therac-20, which operated without significant computer controls, computer software was used to both control and monitor the Therac-25 accelerator.[53]

The software for the Therac-25 was based on modified code from the Therac-6. The software monitored the machine, accepted technician input for specific patient treatment, initialized the machine to administer the defined treatment, and controlled the machine to execute the defined treatment. The machine was enclosed in the patient treatment room to prevent radiation exposure to the technicians. Audio and visual equipment allowed the patient to communicate with the technicians.[54]

A total of 11 Therac-25 machines were installed in the United States and Canada. Over a 19-month period from June 1985 to January 1987, six serious incidents involving the use of the device occurred. In each of the incidents, the patient received an overdose of radiation. Four of the patients died from the overdose, and another eventually had to have both breasts removed and lost use of her right arm as a result of the overdose. A final patient received burns and was only able to fully recover several years after the incident.[55]

Following each incident, AECL was contacted and asked to investigate the situation. However, AECL at first refused to believe that its machine could have been responsible for an overdose. Indeed, following the third incident, AECL responded, “After careful consideration, we are of the opinion that this damage could not have been produced by any malfunction of the Therac-25 or by any operator error.” AECL made some minor changes to the equipment, but because the company did not address the root cause of the problem, additional incidents occurred.[56]

Finally, a physicist at a hospital where two incidents occurred was able to re-create the malfunction and show that the problem was due to a defect in the machine and its software. A failure occurred when a specific sequence of keystrokes was entered by the operator. Because this sequence of keystrokes was nonstandard, the problem rarely occurred and went undetected for a long time. Entry of this combination of keystrokes within a period of eight seconds did not allow time for the beam spreader plate to be rotated into place. The software did not recognize the error, and the patient was then hit with a high-powered electron beam roughly 100 times the intended dose of radiation.[57]

In early 1987, the Food and Drug Administration (FDA) and Health Canada (the Canadian counterpart to the FDA) insisted that all Therac-25 units be shut down. Within the next six months, AECL implemented numerous code changes, installed independent hardware safety locks, and implemented other changes to correct the problem.[58] After these changes, the Therac-25 device continued to be safely used for many years. However, at least three lawsuits were filed against AECL and the hospitals involved in the earlier incidents. The lawsuits were settled out of court, and the results were never revealed.[59]

Discussion Questions

1. What additional measures must be taken in the development of software that, if it fails, can cause loss of human life?
2. What can organizations do to reduce the negative consequences of software development problems in the production of their products and the operation of their business processes and facilities?

End Notes

[1] "Regulation NMS," NASDAQ OMX, www.nasdaqtrader.com/Trader.aspx?id=RegNMS (accessed March 23, 2013).

[2] Columbia Business School, "Press Release: High-Frequency Trading: Is It Good or Bad for Markets?", *Yahoo! Finance*, March 20, 2013, http://finance.yahoo.com/news/high-frequency-trading-good-bad-130000973.html.

[3] Ben Rooney, "Trading Program Sparked May 'Flash Crash,'" *CNN Money*, October 1, 2010, http://money.cnn.com/2010/10/01/markets/SEC_CFTC_flash_crash/index.htm.

[4] Ben Rooney, "Trading Program Sparked May 'Flash Crash,'" *CNN Money*, October 1, 2010, http://money.cnn.com/2010/10/01/markets/SEC_CFTC_flash_crash/index.htm.

[5] BATS Global Markets, "Overview: About Us," www.batsglobalmarkets.com (accessed March 20, 2013).

[6] Melanie Rodier, "Flash Crash at BATS Renews Market Concerns," *Wall Street & Technology*, March 23, 2012, www.wallstreetandtech.com/electronic-trading/flash-crash-at-bats-renews-market-concer/232700195.

[7] D.M. Levine, "Apple Has Mini Flash Crash on BATS," *Huffington Post*, March 23, 2012, www.huffingtonpost.com/2012/03/23/flash-crash-apple-stock-bats_n_1375496.html.

[8] Phil Albinus, "BATS Flash Crash: Here's What Happened," *Advanced Trading*, March 26, 2012, www.advancedtrading.com/exchanges/bats-flash-crash-heres-what-happened/232700223.

[9] Pallavi Gogoi, "Knight Capital Blames Software for Computer Trading Glitch," *USA Today*, August 2, 2012.

[10] Pallavi Gogoi, "Knight Capital Blames Software for Computer Trading Glitch," *USA Today*, August 2, 2012.

[11] Pallavi Gogoi, "Knight Capital Blames Software for Computer Trading Glitch," *USA Today*, August 2, 2012.

[12] Ivy Schmerken, "Another Technical Issue from BATS Rattles Confidence," *Advanced Trading*, January 10, 2013, www.advancedtrading.com/exchanges/another-technical-issue-from-bats-rattle/240146030.

[13] Greg Bensinger, "Software Glitch Mars Nokia's US Re-Entry," *Wall Street Journal* (blog), April 11, 2012, http://blogs.wsj.com/digits/2012/04/11/software-glitch-mars-nokias-us-re-entry-with-att.

[14] "IRS Software Glitch Delays Some Tax Refunds," Reuters, March 3, 2012, www.rawstory.com/rs/2012/03/03/irs-software-glitch-delays-some-tax-refunds.

[15] "Software Glitch Could Strand Chevy Volt Drivers," *Fox News*, October 23, 2012, www.foxnews.com/leisure/2012/10/23/software-glitch-could-strand-chevy-volt-drivers.

[16] Lauren Walsh, "Software Error Prevents Many Georgia Stores from Selling Powerball Tickets," WAGT 26, November 25, 2012, www2.nbc26.tv/news/2012/nov/25/software-error-prevents-many-georgia-stores-sellin-ar-5045240.

[17] Chelsea Bannach, "WSU Software Glitch Stymies Students," *Spokesman-Review*, August 22, 2012, www.spokesman.com/stories/2012/aug/22/wsu-software-glitch-stymies-students.

[18] Katherine Noyes, "Actually, Open Source Code Is Better: Report," *PC World*, February 23, 2012, www.pcworld.com/article/250543/actually_open_source_code_is_better_report.html.

[19] Katherine Noyes, "Actually, Open Source Code Is Better: Report," *PC World*, February 23, 2012, www.pcworld.com/article/250543/actually_open_source_code_is_better_report.html.

[20] Klaus Enzenhofer, "Mobile App Performance – How to Ensure High Quality Experiences," *Testing Experience*, September 19, 2012, www.testingexperience.com/testingexperience19_09_12.pdf.

[21] Cem Kaner, "Quality Cost Analysis: Benefits and Risks," *Software Quality Assurance* 3, no. 1 (1996), www.kaner.com/pdfs/Quality_Cost_Analysis.pdf (accessed March 23, 2013).

[22] Paul Bibby, "Qantas Exposed to Compo Claims," *WA Today,* October 9, 2008, www.watoday.com.au/national/qantas-exposed-to-compo-claims-20081009-4x6t.html.

[23] 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).

[24] Barry W. Boehm, "Improving Software Productivity," *IEEE Computer* 20, no. 8 (1987): 43–58.

[25] Capers Jones, *"Software Quality in 2002: A Survey of the State of the Art,"* Software Productivity Research, Inc., November 2002.

[26] Dennis R. Goldenson and Diane L. Gibson, "Demonstrating the Impact and Benefits of CMMI: An Update and Preliminary Results," October 2003, www.sei.cmu.edu/reports/03sr009.pdf.

[27] Northrup Grumman, "Press Release: Northrop Grumman's Rolling Meadows Campus Achieves CMMI(R) Maturity Level 5 Rating," *Globe Newswire*, December 21, 2012, www.irconnect.com/noc/press/pages/news_releases.html?d=10016400.

[28] Jonathan P. Bowen, "The Ethics of Safety-Critical Systems," *Communications of the ACM* 43 (2000): 91.

[29] "NASA, USAF, JPL Announce Mariner I Lost Because Flight Control Computer Generated Incorrect Steering Commands," *New York Times*, July 28, 1962.

[30] Peter B. Ladkin and Mike Beims, "The Chinook Crash," *The Risks Digest (blog),* January 10, 2002, http://catless.ncl.ac.uk/Risks/21.20.html#subj7.

[31] Matt Lake, "Epic Failures: 11 Infamous Software Bugs," *New Zealand PC World*, September 27, 2010, http://pcworld.co.nz/pcworld/pcw.nsf/feature/epic-failures-11-infamous-software-bugs-p8.

[32] RideAccidents.com, "Disneyland Faulted for Big Thunder Mountain Railroad Collision – Again," www.rideaccidents.com/2004.html#aug27b.

[33] "Surge Caused Fire in Rail Car," *Washington Times*, April 27, 2007, www.washingtontimes.com/news/2007/apr/12/20070412-104206-9871r.

[34] Ryan Witt, "Map of U.S. Nuke Reactors Reveals What Happened in Japan Could Happen in America," *Examiner,* March 14, 2011, www.examiner.com/political-buzz-in-national/could-japan-s-nuclear-crisis-happen-the-united-states.

[35] George C. Wilson, "Navy Missile Downs Iranian Jetliner," *Washington Post,* July 4, 1988, www.washingtonpost.com/wp-srv/inatl/longterm/flight801/stories/july88crash.htm.

[36] "ISO Certifications Top One Million Mark: Food Safety and Information Security Continue Meteoric Increase," *ISO News*, October 25, 2010, www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1363.

[37] Oliver Mackel, "Software FMEA: Opportunities and Benefits in the Development Process of Software-Intensive Technical Systems," www.fmeainfocentre.com/papers/mackel1.pdf (accessed May 3, 2013).

[38] Raytheon, "Our Company," www.raytheon.com/ourcompany (accessed March 28, 2013).

[39] Raytheon, "Enhance the Value You Provide to Raytheon and Our Customers," www.raytheon.com/connections/supplier/r6s/fmea/index.html (accessed March 28, 2013).

[40] InterSystems Corporation, "About Us: Company Profile," www.intersystems.com/aboutus/index.html (accessed March 30, 2013).

[41] InterSystems Corporation, "Press Release: InterSystems Corporation Achieves ISO 9001:2008 Certification," January 5, 2012, www.intersystems.com/press/2012/ISO_9001.html.

[42] InterSystems Corporation, "Press Release: InterSystems Corporation Achieves ISO 9001:2008 Certification," January 5, 2012, www.intersystems.com/press/2012/ISO_9001.html.

[43] InterSystems Corporation, "Case Studies: Johns Hopkins Kimmel Cancer Center Leverages Caché Performance and Efficiency to Enable Optimal Cancer Treatment," www.intersystems.com/casestudies/cache/johns_hopkins.html (accessed April 1, 2013).

[44] Ingrid Lunden, "App Stores in Q1 2013 Hauled in $2.2 B in Sales on 13.4B Downloads, Google/Apple Duopoly Leading the Way: Canalys," *Tech Crunch*, April 8, 2013,

http://soylaostia.com/2013/04/app-stores-in-q1-2013-hauled-in-2-2b-in-sales-on-13-4b-downloads-googleapple-duopoly-leading-the-way-canalys-ingrid-lundentechcrunch.

[45] "Apple Publishes Guidelines for App Approval," *CBS News,* September 9, 2010, www.cbsnews.com/stories/2010/09/09/tech/main6850597.shtml.

[46] Fred von Lohmann, "Another iPhone App Banned: Apple Deems South Park 'Potentially Offensive,'" Electronic Frontier Foundation, February 17, 2009, www.eff.org/deeplinks/2009/02/south-park-iphone-app-denied.

[47] "Apple Publishes Guidelines for App Approval," *CBS News*, September 9, 2010, www.cbsnews.com/stories/2010/09/09/tech/main6850597.shtml.

[48] "Apple Publishes Guidelines for App Approval," *CBS News*, September 9, 2010, www.cbsnews.com/stories/2010/09/09/tech/main6850597.shtml.

[49] Lauren Acurantes, "Google Removes 21 Bad Apps from Android Market," *Manila Bulletin Online,* March 2, 2011, www.mb.com.ph/articles/307060/google-removes-21-bad-apps-android-market.

[50] "Apple Publishes Guidelines for App Approval," *CBS News*, September 9, 2010, www.cbsnews.com/stories/2010/09/09/tech/main6850597.shtml.

[51] "Apple Opens iOS to Third-Party Dev Tools, Reveals Approval Guidelines," *AppleInsider*, September 9, 2010, www.appleinsider.com/articles/10/09/09/apple_no_longer_banning_third_party_ios_development_tools.html.

[52] ComputingCases.org, "Therac History, Genesis of the Therac-25," www.computingcases.org/case_materials/therac/supporting_docs/levenson/Therac%20History.html (accessed April 1, 2013).

[53] ComputingCases.org, "Therac History, Genesis of the Therac-25," www.computingcases.org/case_materials/therac/supporting_docs/levenson/Therac%20History.html (accessed April 1, 2013).

[54] Troy Gallagher, "Therac-25 Computerized Radiation Therapy," http://kellyhs.org/itgs/ethics/reliability/THERAC-25.htm (accessed April 1, 2013).

[55] Nancy Levenson and Clark S. Turner, "An Investigation of the Therac-25 Accidents," www.onlineethics.org/cms/4661.aspx (accessed April 1, 2013).

[56] Nancy Levenson and Clark S. Turner, "An Investigation of the Therac-25 Accidents," www.onlineethics.org/cms/4661.aspx (accessed April 1, 2013).

[57] Troy Gallagher, "Therac-25 Computerized Radiation Therapy," http://kellyhs.org/itgs/ethics/reliability/THERAC-25.htm (accessed April 1, 2013).

[58] "A History of Introduction and Shut Down of Therace-25," www.computingcases.org/case_materials/therac/case_history/Case%20History.html (accessed April 1, 2013).

[59] Nancy Levenson and Clark S. Turner, "An Investigation of the Therac-25 Accidents," www.onlineethics.org/cms/4661.aspx (accessed April 1, 2013).

CHAPTER 8

THE IMPACT OF INFORMATION TECHNOLOGY ON PRODUCTIVITY AND QUALITY OF LIFE

QUOTE

It is dangerously destabilizing to have half the world on the cutting edge of technology while the other half struggles on the bare edge of survival.
—President Bill Clinton

VIGNETTE

Problems with the E-Rate Program

In March 2013, Democratic Senator John D. Rockefeller IV of West Virginia, chair of the Senate Commerce Committee, called for an expansion of the Education Rate (E-Rate) program, which provides money to connect schools and libraries to the Internet. The E-Rate program is overseen by the Federal Communications Commission (FCC) and is funded by fees charged to telecommunication companies. Those companies may, in turn, pass those charges along to their customers in the form of a "Universal Service" charge. The E-Rate program is administered by the Universal Service Administrative Company (USAC), a private nonprofit set up by the FCC. When the program started in 1996, only 14 percent of classrooms and 28 percent of public libraries in the United States were

connected to the Internet. Today, over 92 percent of classrooms and virtually 100 percent of public libraries have Internet access.[1,2] Rockefeller argued that the program should now be used to introduce high-speed, 1-gigabit Internet connections into every school in the United States.[3]

Rockefeller's proposal came just a year after a federal district court sentenced Gloria Harper, the owner of two information technology companies, to 30 months in prison for bribing school officials to win lucrative E-Rate contracts. Harper had offered kickbacks to employees of schools in Illinois, Arkansas, Florida, and Louisiana. In return, those employees helped ensure that contracts for IT services at those schools were awarded to Harper's companies. In addition to being sentenced to prison, Harper was fined $40 million. Xavier University Preparatory School in New Orleans and the Eagle School District in Arkansas were each denied E-Rate funding of $22,000 as a result of the scheme.[4,5] The scandal was not an isolated event. Gloria Harper is, in fact, one of 44 individuals or companies that have been convicted of E-Rate fraud since 2003.[6]

Following a yearlong investigation, a House subcommittee in 2005 approved a bipartisan staff report detailing abuse, fraud, and waste in the E-Rate program. In one infamous example, USAC disbursed $101 million between 1998 and 2001 to provide high-speed Internet access to over 1,500 schools in Puerto Rico, but a subsequent review found that very few computers were ever connected to the Internet. In fact, $23 million worth of equipment was found in unopened boxes in a warehouse. Eventually, the former Puerto Rican secretary of education was found guilty of fraud, sentenced to three years in prison, and fined $4 million.[7]

In November 2010, the U.S. Department of Justice settled two lawsuits for a total of $16.25 million against Hewlett-Packard (HP) in connection with the awarding of E-Rate technology and service contracts in the Dallas (DISD) and Houston Independent School Districts (HISD). The lawsuits alleged that between 2002 and 2005 contractors working with HP offered bribes in order to win very

profitable contracts that included some $17 million in HP equipment.[8] In 2006, HP banned the two resellers who were under investigation from selling its equipment. The two companies allegedly provided illegal inducements in the form of the use of a private yacht, sporting tickets, and other gifts to school district employees while the companies were bidding on the DISD and HISD E-Rate program contracts.[9]

In 2008, the former chief technology officer of DISD and the former chief executive officer of MSE were found guilty of bribery for illegal conduct relating to the DISD contract. They were each sentenced to over a decade in prison. In 2009, the DISD was fined $750,000 and agreed to drop its requests for more than $150 million in federal funding.[10] The HISD was fined $850,000.[11]

Just as the U.S. Department of Justice was handing down its ruling in the HP case, the General Accounting Office (GAO)—the investigative arm of Congress—released a report stating that the internal controls the FCC and USAC had established for the E-Rate program were lacking. These controls were set up to help the USAC make decisions about which institutions to fund, review payments made to the institutions, and audit the institutions to make sure they are complying with E-Rate rules. For instance, to qualify for E-Rate funds, applicants must go through a 39-step procedure. In addition, the USAC created a special team to review allegations of fraud that originate from the Whistleblower Hotline, law enforcement investigations, press reports, and the FCC Office of Inspector General audits. However, the E-Rate program continues to face challenges in ensuring that its participating institutions are complying with the various E-Rate rules designed to prevent fraud and waste. To review compliance to these rules, the USAC contracts with independent public accountants to conduct audits of E-Rate participants.[12] The USAC commissions between 100 and 150 audits per year.[13] However, USAC has no documented and approved policies for the audit procedure. More importantly, the GAO determined that USAC was not effectively using the information it gained from

these audits. Of 64 program participants who were audited more than once over a three-year period, 36 had repeated the same rule violation. This may in part be a consequence of delays in the audit process. The GAO found that an average of 224 days passed between the submission of a draft audit and its final approval.[14]

The GAO recommended that the USAC conduct a detailed audit of its internal controls. As a result, USAC created a request for proposals and began the process of evaluating the proposals through a competitive bidding process.[15] However, by March 2013, when Senator Rockefeller proposed that the E-Rate program be expanded to offer higher-speed Internet to every school in the United States, USAC had yet to announce the awarding of a contract for the auditing of its internal controls.

Questions to Consider

1. What are the key points from this case that apply to anyone who is involved in competing for or awarding contracts for products or services?
2. Imagine you are a salesperson who will be awarded over $1 million in commissions if your firm is awarded a major contract. What ethical actions can you take to ensure that you and your firm are viewed favorably by the key decision maker in the deal?
3. What weaknesses exist in USAC's internal control procedures? Should these weaknesses prevent the government from expanding the program?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What impact has IT had on the standard of living and worker productivity?
2. What is being done to reduce the negative influence of the digital divide?
3. What impact can IT have on improving productivity by reducing costs and/or improving quality?
4. What ethical issues are raised because some entities can afford to make significant investments in IT while others cannot and thus are blocked in their efforts to raise productivity and quality?

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.[16] By way of comparison, during the latest recession in the United States (which began in 2007), the GDP growth rate declined by 6.8 percent during the fourth quarter of 2008[17] and the U.S. unemployment rate hit a peak of 10.2 percent in October 2009.[18]

IT Investment and Productivity

Productivity is defined as the amount of output produced per unit of input, and it is measured in many different ways. For example, productivity in a factory might be measured by the number of labor hours it takes to produce one item, while productivity in a service sector company might be measured by the annual revenue an employee generates divided by the employee's annual salary. Most countries have been able to produce more goods and services over time—not through a proportional increase in input 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 Bureau of Labor Statistics tracks U.S. productivity on a quarterly basis. In the United States, labor productivity growth has averaged about 2 percent per year for the past century, meaning that living standards have doubled about every 36 years.[19]

Figure 8-1 shows the annual change in U.S. nonfarm labor productivity since 1947. The increase in productivity averaged 2.8 percent per year from 1947 to 1973 as modern management techniques and automated technology 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 from 2007 to 2012, a period of time corresponding to the deepest recession in the United States since the Great Depression.

Innovation is a key factor in productivity improvement, and IT has played an important role in enabling innovation. Progressive management teams 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.

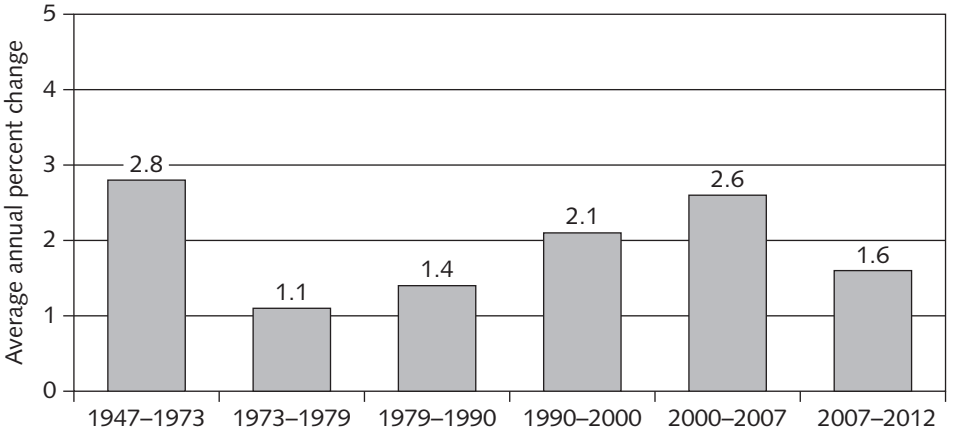


FIGURE 8-1 U.S. nonfarm labor productivity, 1947–2012
Source Line: U.S. Bureau of Labor Statistics, "Labor Productivity and Costs, 1947–2012," www.bls.gov/lpc/prodybar.htm.

Today, organizations are trying to further improve IT systems and business processes that have already gone through several 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, such as the BlackBerry®, Droid®, and iPhone®. 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 respond to 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 productivity rate should have decreased.[20]

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 IT investment to result in a significant increase in productivity.[21]

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/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 try directly to 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
Improving performance by becoming more efficient	Selling more goods to increase capacity and use of existing resources

Source Line: Course Technology/Cengage Learning.

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 firms 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 with many other industrialized nations. This flexibility makes it easier for 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.
- In today's service-based economy, it is difficult to measure the real output of such services as accounting, customer service, and consulting.
- IT investments don't always yield tangible results, such as cost savings and reduced head count; instead, many produce intangible benefits, such as improved quality, reliability, and service.

As you can see, it is difficult to 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.

Telework

Telework (also known as telecommuting) is a work arrangement in which an employee works away from the office—at home, at a client's office, in a hotel—literally, anywhere. In telework, an employee uses various forms of electronic communication, including texting, email, audio and videoconferencing, and online chat. Teleworkers access the Internet via smartphones, tablets, laptops, and similar devices to retrieve computer files; log on to software applications; access corporate databases; and communicate with fellow employees, managers, customers, and suppliers. The goal of telework is to allow employees to be effective and productive from wherever they are. According to the U.S. Bureau of Labor Statistics, 21 percent of employed Americans worked at least some hours at home each week during 2010.[22] Another study found that between 20 and 30 percent of Americans worked from home at least one day a week during 2011.[23]

Factors that have increased the prevalence of telework include advances in technology that enable people to communicate and access the Internet from almost anywhere, the increasing number of broadband connections in homes and retail locations, high levels of traffic congestion, rising gasoline prices, and growing concern over the effects of automobile CO^2 emissions. Another key factor is that increasingly scarce and highly trained workers frequently demand more flexible work arrangements, including flex hours and the ability to occasionally work from home.

A number of states and the federal government have passed laws to encourage telework. For example, Virginia set a goal in 2008 of having 20 percent of eligible state workers teleworking by 2010. The state met the goal and now has over 8,500 workers telecommuting out of 25,000 eligible employees (34 percent).[24] The Telework Improvement Act of 2010 makes all federal employees eligible to telework one day per week (unless their manager determines they are ineligible for telework). About 21 percent of eligible federal employees telework.[25]

However, not all organizations are fully supportive of telework. Several organizations, including Bank of America, Best Buy, and Yahoo!, have recently cut back their telework program for employees for a variety of reasons, including the need to cut costs, improve efficiency, and encourage greater collaboration among employees.[26,27,28]

Organizations should prepare guidelines and policies to define the types of positions and workers who represent ideal telework opportunities. Clear guidelines must be set for how and when work will be given to and collected from teleworkers. If there are certain hours during which the teleworker must be available, these too must be defined. Employee work expectations and performance criteria must also be delineated.

A Sensis® Consumer Report found that while the majority of teleworkers (62 percent) were positive about teleworking, nearly 25 percent felt teleworking had no real impact on their lives, and 13 percent of teleworkers reported a negative impact. The negative feelings were primarily because workers felt that teleworking had not really improved their productivity. In addition, many teleworkers felt that there was increased pressure to work outside the normal business hours so that they now worked longer hours, thus taking time away from their families.[29] Another recent study concluded that telework has led to an expansion of work hours beyond the standard workweek and has placed additional demands on salaried workers.[30]

Some positions—such as management positions or those in which face-to-face communication with other employees or customers is required—may not be well suited for telework. In addition, some individuals are not good candidates for teleworking.

Telework opportunities need to be weighed based on the characteristics of the individual as well as the requirements of the position. Table 8-2 and Table 8-3 list some of the advantages and disadvantages of telework from the perspectives of employees and organizations, respectively.

TABLE 8-2 Advantages/disadvantages of teleworking for employees

Advantages	Disadvantages
People with disabilities who otherwise find public transportation and office accommodations a barrier to work may now be able to join the workforce.	Some employees are unable to be productive workers away from the office.
Teleworkers avoid long, stressful commutes and gain time for additional work or personal activities.	Teleworkers may suffer from isolation and may not really feel "part of the team."
Telework can reduce the need for employees to take time off to stay home to care for a sick family member.	Workers who are out of sight also tend to be out of mind. The contributions of teleworkers may not be fully recognized and credited.
Teleworkers have an opportunity to experience an improved work/family balance.	Teleworkers must guard against working too many hours per day because work is always there.
Telework reduces ad hoc work requests and disruptions from fellow workers.	The cost of the necessary equipment and communication services can be considerable if the organization does not cover these.

Source Line: Course Technology/Cengage Learning.

TABLE 8-3 Advantages/disadvantages of teleworking for organizations

Advantages	Disadvantages
As more employees telework, there is less need for office and parking space; this can lead to lower costs.	Allowing teleworkers to access organizational data and systems from remote sites creates potential security issues.
Allowing employees to telework can improve morale and reduce turnover.	Informal, spontaneous meetings become more difficult if not impossible.
Telework allows for the continuity of business operations in the event of a local or national disaster and supports national pandemic-preparedness planning.	Managers may have a harder time monitoring the quality and quantity of the work performed by teleworkers, wondering, for instance, if they really "put in a full day."
The opportunity to telework can be seen as an additional perk that can help in recruiting.	Increased planning is required by managers to accommodate and include teleworkers.
There may be an actual gain in worker productivity.	There are additional costs associated with providing equipment, services, and support for people who work away from the office.
Telework can decrease an organization's carbon footprint by reducing daily commuting.	Telework increases the potential for lost or stolen equipment.

Source Line: Course Technology/Cengage Learning.

The Digital Divide

When people talk about standard of living, they are often referring to a level of material comfort measured by the goods, services, and luxuries available to a person, group, or nation—factors beyond the GDP-based measurement of standard of living. Some of these indicators include the following:

- Average number of calories consumed per person per day
- Availability of clean drinking water
- Average life expectancy
- Literacy rate
- Availability of basic freedoms
- Number of people per doctor
- Infant mortality rate
- Crime rate
- Rate of home ownership
- Availability of educational opportunities

Another indicator of standard of living is the availability of information and communications technology. The **digital divide** is a term used to describe the gulf between those who do and those who don't have access to modern information and communications technology, such as cell phones, smartphones, personal computers, and the Internet. There are roughly 2.4 billion Internet users worldwide, but the worldwide distribution of Internet users varies greatly from region to region.

The digital divide exists from country to country (see Table 8-4) and even within countries—among age groups, economic classes, and people who live in cities versus those in rural areas. For example, in India, while 20 percent of urban Indians are connected to the Internet, only 3 percent of rural Indians are connected.[31] In the United States, Hispanics and African Americans, adults living in poor households, and senior citizens are least likely to have Internet access.[32]

TABLE 8-4 High-low Internet penetration by country within region

Region	Country with the highest Internet penetration	% of population	Country with the lowest Internet penetration	% of population
Africa	Morocco	51%	Ethiopia	1%
Americas	Falkland Islands	96%	Belize	23%
Asia	South Korea	82%	Myanmar	1%
Europe	Monaco	100%	Kosovo	20%
Middle East	Qatar	86%	Iraq	7%
Oceania/Australia	Australia	89%	Papua New Guinea	2%

Source Line: Internet World Stats, www.internetworldstats.com/stats.htm.

Many people believe that the digital divide must be bridged for a number of reasons. Clearly, health, crime, and other emergencies could be resolved more quickly if a person

in trouble had easy access to a communications network. Access to IT and communications technology can also greatly enhance learning and provide a wealth of educational and economic opportunities as well as influence cultural, social, and political conditions. Much of the vital information people need to manage their career, retirement, health, and safety is increasingly provided by the Internet.

The E-Rate program discussed in the opening vignette was designed to help eliminate the digital divide within the United States. This program and others designed to increase the availability of low-cost computers, cell phones, and smartphones are discussed in the following sections.

E-Rate Program

The **Education Rate (E-Rate) program** was created through the Telecommunications Act of 1996. The full name of the program is The Schools and Libraries Program of the Universal Service Fund. E-Rate helps schools and libraries obtain broadband Internet services to advance the availability of educational and informational resources. The program provides cost discounts that range from 20 percent to 90 percent for eligible telecommunications services, depending on location (urban or rural) and economic need. (Economic need is determined by percentage of students eligible for participation in the National School Lunch Program.)

E-Rate reimburses telecommunications, Internet access, and internal connections providers for discounts on eligible services provided to schools and libraries. Schools and libraries must apply for the discounts, and the USAC works with the service providers to make sure that the discounts are passed along to program participants.

While the program has steadily increased the number of schools and libraries connected to the Internet, there have been problems with fraud, as detailed in the opening vignette. In addition, the benefits delivered by the program have been called into question. A University of Chicago study examined the impact of the E-Rate program in California and found that the number of students in poor schools going online had indeed increased dramatically. However, the study found no evidence that the program had any effect on students' performance on any of the six subjects (math, reading, science, language, spelling, and social studies) covered in the Stanford Achievement Test. Researchers concluded that either the schools did not know how to make effective use of the Internet or that Internet use was simply not a productive way to boost test scores.[33] Despite the fraud and lack of evidence of a positive impact on student test scores, the $2.3 billion per year E-Rate program continues today.

Low-Cost Computers

As noted above, it is estimated that as of June 2012, nearly 2.4 billion people worldwide have access to the Internet.[34] Although that number is impressive, it still leaves nearly 5 billion people (72 percent of the world's population) unconnected. What most of those 5 billion people have in common is low income. Increasing the availability of low-cost computers can help reduce the digital divide.

One Laptop per Child (OLPC)

The nonprofit organization **One Laptop per Child (OLPC)** has a goal of providing children around the world with low-cost laptop computers to aid in their education. As of 2013, the program has worked with federal, state, and local governments to help distribute over

2.4 million low-cost computers to students in 40 countries.[35] The first version of its laptop, the OLPC XO, was made available to third-world countries in 2007 and came with a hand crank for generating power in places where electricity is not readily available. It was distributed at a cost of around $200. The current version of the OLPC is the XO-4 (see Figure 8-2), which was designed to require just 1 watt of electricity per hour and sell for $206, with a minimum purchase of 10,000 units. The machine comes with up to an 8 GB hard drive and 1.2 GHz processor.[36] The computer runs a Linux-based operating system and comes with a suite of 300 or so learning applications called Sugar. The computer can connect to the Internet via wireless or satellite communications.[37]

FIGURE 8-2 The OLPC XO-3 tablet computer
Credit: Courtesy of fuseproject.

Nepal is one of the poorest countries in the world, with an average annual per capita income of about $475 (USD)[38] and an unemployment rate of 46 percent.[39] Much of its rural population has limited access to even the most basic of social services. The OLPC program in Nepal started in 2008 as a small pilot project in two schools. Within three years, it expanded to 32 schools with a total enrollment of 3,300 students in grades 2 to 6. The goal of the program in Nepal is to improve the quality of education and the access to instructional materials. Some 180 teachers are learning how to integrate the technology into their teaching practices and developing curriculum-based computer educational activities. The OLPC program in Nepal has shown that technology-based education can be successfully introduced into rural schools using prepared local teachers already in the school system.[40]

Classmate+

In 2006, Intel introduced a low-cost laptop called the Classmate PC. The first generation of this notebook computer cost under $400 and was designed for use in kindergarten through high school classrooms in developing countries.[41] The computer began shipping in early

2007 to 25 countries, including Brazil, Chile, Nigeria, China, India, and Vietnam.[42] Since then, Intel and Lenovo have partnered to introduce the Classmate+ laptop, targeted for sale in bulk quantities to educational institutions and agencies in third-world countries. Some Classmate models are the traditional clamshell style, while others are convertible tablet-style machines. Intel does not actually build the machine but instead provides the basic design used by various manufacturers around the world. Over 4 million Classmate computers have been deployed globally.[43] The Classmate has a 10-inch screen, runs the Windows 7 or Linux operating system, comes with 1 or 2 GB of RAM, has a built-in camera, and has wireless capability. The laptop comes equipped with the Intel Learning Series Software Suite of educational software.[44]

Raspberry Pi

The Raspberry Pi is a small (about the size of a credit card), inexpensive ($25–$35) computer developed by the Raspberry Pi Foundation, a United Kingdom charity. This stripped-down computer comes with either 256 MB or 512 MB of RAM, a 700 MHz processor, one or two USB ports, and an Ethernet port—but no case and no monitor. The computer, which runs the Linux operating system, was designed to teach computer programming to young children, and as an alternative, low-cost desktop computer replacement for those willing to try new technology.[45,46] Although the price of the Pi certainly makes it attractive, it is not clear that this device has the necessary ruggedness, portability, and functionality to meet the educational computing needs of schoolchildren. The quantity of these computers to be manufactured remains to be seen.

Mobile Phone: The Tool to Bridge the Digital Divide?

Some industry observers identify the increasing use of cell phones as an important first step in bridging the digital divide in many countries. The rapid and widespread use of cell phones has resulted in an increased investment in the infrastructure required to support wireless communications. In addition, as cell phone use has spread, financial institutions and other organizations have built applications capable of accepting text-based input to process user transactions and store cash or credits on users' phones.

In almost all countries, many more people have access to cell phones than they do computers. Cell phones have several advantages over personal computers, including the following:

- Cell phones come in a wide range of capabilities and costs, but are cheaper than personal computers. Some users simply purchase a SIM card (essentially a memory chip that holds the owner's account information, including his or her phone number and contacts information), and then swap SIM cards in and out of a shared cell phone to lower the costs even further.
- Cell phones are more portable and convenient than the smallest laptop computer.
- Cell phones come with an extended battery life (much longer than any personal computer battery), which makes the cell phone more reliable in regions where access to electricity is inadequate or nonexistent.
- There is almost no learning curve required to master the use of a cell phone.
- Basic cell phones require no costly or burdensome applications that must be loaded and updated.
- There are essentially no technical-support challenges to overcome when using a cell phone.

For many people who can afford it, the next step in bridging the digital divide is the acquisition of a smartphone—complete with an operating system capable of running applications and providing access to the Internet. As the cost of the technology and monthly usage fees decrease, even more people will be able to make this upgrade, and when they do, they will gain access to thousands of applications and Web sites that they can use for business, educational, and personal purposes.

When IT is available to everyone—regardless of economic status, geographic location, language, or social status—it can enhance the sharing of ideas, culture, and knowledge. How much will the benefits of IT raise the standard of living in underdeveloped countries? Could the end of the digital divide change the way people think about themselves in relation to the rest of the world? Could such enlightenment, coupled with a better standard of living, contribute to a reduction in violence, poverty, poor health, and even terrorism?

THE IMPACT OF IT ON HEALTHCARE COSTS

The rapidly rising cost of health care is one of the twenty-first century's major challenges. U.S. healthcare spending hit an estimated $2.7 trillion in 2011 and is expected to increase an average of 6.3 percent per year (a rate much higher than overall inflation) between 2015 and 2021, according to the Centers for Medicare and Medicaid Services.[47] Much of this growth is due to the continued aging of the population in the United States and the rise in healthcare expenditures per person. The development and use of new medical technology, such as new diagnostic procedures and treatments (see Figure 8-3), account for much of the increase in healthcare spending per person in excess of general inflation.[48,49,50] Although many new diagnostic procedures and treatments are at least moderately more effective than their older counterparts, they are also more costly. 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.

Patients sometimes overuse medical resources that appear to be free or almost free thanks to the share of medical bills that is paid by third parties, such as insurance companies and government programs. A patient who doesn't have to pay for a medical test or procedure is probably less likely to consider its cost-to-benefit ratio. Attempts by insurance companies to rein in those costs have led to a blizzard of paperwork but have proven largely ineffective.

To really gain control over soaring healthcare costs, patient awareness must be raised and technology costs must be managed more carefully. In the meantime, however, the improved use of IT in the healthcare industry can lead to significant cost reductions in a number of ways.

Electronic Health Records

Although the healthcare industry depends on highly sophisticated technology for diagnostics and treatment, it was slow to implement IT solutions to improve productivity and efficiency. As of 2005, the healthcare industry only invested about $3,000 in IT for each worker, compared with about $7,000 per worker in private industry generally, and nearly $15,000 per worker in the banking industry. However, the healthcare industry has now greatly increased its investment in IT— spending over $88 billion in 2010 alone to

FIGURE 8-3 The development and use of new technology has contributed to increased healthcare spending
Credit: © Farferros/Shutterstock.com

implement electronic health records (EHRs), convert to a new coding system (known as ICD-10) for diagnosis and inpatient codes, and begin use of a new Food and Drug Administration Web portal to report deaths and injuries caused by medical devices.[51]

Using IT to capture and record patient data provides a significant opportunity for improving health care and increasing productivity. Before seeing a physician, many patients are given a clipboard and pen with a standard form to complete. Some people must wonder: "This is the same form I filled out last time; what did they do with the data from my last visit?"

It can be extremely difficult to pull together the paper trail created by a patient's interactions with various healthcare entities to create a clear, meaningful, consolidated view of that person's health history. In some cases, medical personnel are simply unable to locate paper medical records. This lack of patient data transparency can result in diagnostic and medication errors as well as the ordering of duplicate tests, which dramatically increase healthcare costs. It can even compromise patient safety. For example, emergency room physicians must often treat patients who are unconscious and incapable of providing essential medical information, such as the name of his or her primary care physician, information about recent illnesses or surgeries, medications taken, allergies, and other useful data. Without such data, an emergency room physician is essentially taking a gamble in treating that patient. If the United States had a comprehensive healthcare information network, such medical data could be readily available for all patients at any medical facility. Some studies have estimated that over 98,000 people die in hospitals each

year due to preventable medical mistakes.[52] As far back as 2004, healthcare experts agreed that "going digital" could eliminate many of these needless deaths.

An **electronic health record (EHR)** is a computer-readable record of health-related information on an individual. 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. Data in an EHR can then be easily accessed by other healthcare professionals. See Figure 8-4.

FIGURE 8-4 An EHR is a computer-readable record of health-related information on an individual
Credit: Courtesy of U.S. Department of Veterans Affairs.

The **Health Information Technology for Economic and Clinical Health Act (HITECH Act)** was passed as part of the $787 billion 2009 American Recovery and Reinvestment Act economic stimulus plan. HITECH is intended to increase the use of health information technology by (1) requiring the government to develop standards for the nationwide electronic exchange and use of health information; (2) providing $20 billion in incentives to encourage doctors and hospitals to use EHR to electronically exchange patient healthcare data; (3) saving the government $10 billion through improvements in the quality of care, care coordination, reductions in medical errors, and duplicate care; and (4) strengthening the protection of identifiable health information. Under this act, increased Medicaid or Medicare reimbursements will be made to doctors and hospitals that demonstrate "meaningful use" of EHR technology. Meaningful use is defined as EHR technology that enables a hospital to prescribe electronically, exchange data with other providers, and generate certain "clinical quality measure" reports.[53]

The PricewaterhouseCoopers LLP Health Research Institute estimated that a 500-bed hospital could receive $6.1 million in HITECH incentives to purchase, deploy, and

maintain an EHR system. On the other hand, failure to implement such a system by 2015 could cause the hospital to lose $3.2 million in funding annually, depending on the hospital's volume of Medicare, Medicaid, and charity-care patients. Adoption of basic EHR systems—which include a set of basic EHR functions, including clinician notes—at nonfederal acute-care hospitals has increased nearly fivefold from 2008 to 2012. The percentage of hospitals in possession of a certified EHR system is also rising. A certified EHR is EHR technology that has been certified as meeting federal requirements for some or all of hospital objectives for meaningful use. See Figure 8-5.[54]

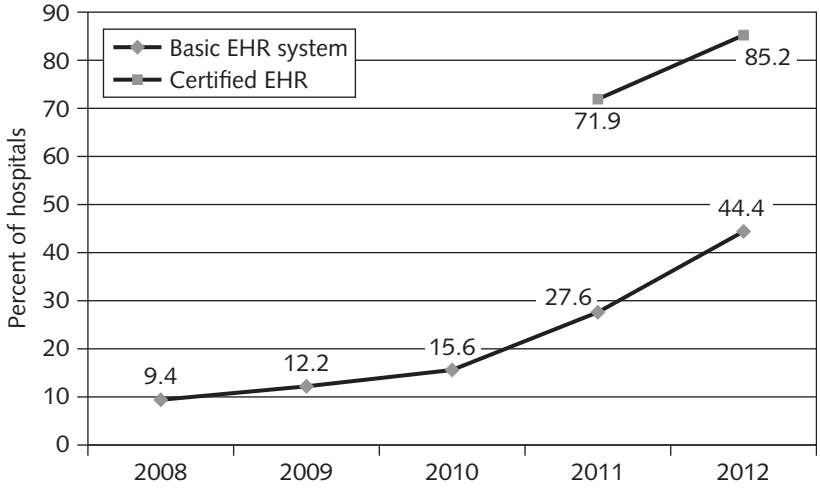


FIGURE 8-5 Percent of nonfederal acute-care hospitals with adoption of at least a basic EHR system and those in possession of a certified EHR

Source Line: Dustin Charles, MPH; Jennifer King, PhD; Vaishali Patel, PhD; Michael F. Furukawa, PhD, "Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2012," ONC Data Brief No. 9.

Individual physicians are eligible to receive as much as $44,000 under Medicare and $63,750 under Medicaid for the implementation and meaningful use of EHR systems. To meet the meaningful use requirement, physicians must be able to demonstrate that they are using certified EHR technology in ways that lead to significant and measurable results in achieving health and efficiency improvements, such as e-prescribing of medications and treatments, electronic exchange of health information, and electronic submission of clinical quality data.[55]

HITECH also attempts to improve federal privacy and security measures safeguarding health information. It requires that individuals be notified if there is any unauthorized use of their health information, allows patients to request an audit trail showing all disclosures of their health information via electronic means, requires health providers to gain authorization from patients to use their health information for marketing and fund-raising activities, and increases penalties for violations and provides greater resources for enforcement and oversight activities.[56]

In 2005, RAND Corporation predicted that if the American healthcare system broadly adopted the use of EHR systems, healthcare costs would decline by over $81 billion per year and the quality of health care would rise.[57] This prediction stimulated a major increase in investment in EHR and stimulated the federal government to award billions

of dollars through the HITECH program as an incentive for physicians and hospitals to implement such systems.

With the benefit of 20/20 hindsight, the RAND forecasts have proven to be overly optimistic. There is little evidence of any savings—with overall healthcare costs actually increasing $800 billion since the 2005 report. As far as improving the quality of health care, there is also a lack of solid evidence. A second study published by the RAND Corporation in late 2010, involving half the acute-care hospitals in the United States, found that except for basic systems used to treat congestive heart failure patients, EHRs are not improving process of care measures for many large hospitals.[58] Another opinion on the value of EHR comes from David Kibbe, a physician and technology advisor to the American Academy of Family Physicians, who wrote that "electronic records are notoriously expensive and difficult to implement." He went on to note that we still do not have conclusive evidence that the use of EHRs improves the quality of patient care.[59]

EHR skeptics point out that the rate of adoption of EHR systems has been slower than expected, and that the systems are often difficult to use. Critics also point out that most EHR systems do not allow care providers to share patient information across different vendors' systems. Some critics believe that the use of EHR may actually have contributed to increased healthcare costs by making it easier to bill for patient services.[60] On the other hand, some physicians believe that the data collected by the government through EHR reporting will be used to justify a decrease in their Medicare and Medicaid reimbursements.[61]

The cost to implement EHR systems is a concern for both large and small medical providers. A typical three-physician practice would need to spend between $173,000 and $296,000 to purchase and maintain an EHR system, while a larger medical institution could easily spend millions of dollars to fully implement an EHR system.[62] For example, Wake Forest Baptist Medical Center, an academic medical center with 1,004 acute-care and rehabilitation beds, and over 13,000 employees, has been in the process of implementing an EHR system for years and recently reported $13.3 million in expenses related directly to those efforts.[63] It also reported an additional $8 million in implementation expenses, due in part to the handling of fewer operating-room cases because surgeons had to spend time learning the new system.[64]

One cannot help but wonder where we will be in 10 years in terms of healthcare spending. Will we have made a meaningful reduction in the number of avoidable deaths? Will we have earned a worthwhile return on the investment in EHR? Are those who are advocating the adoption of EHR acting ethically or are they pushing some other agenda?

Use of Mobile and Wireless Technology in the Healthcare Industry

Although slow to invest in IT, the healthcare industry was actually a leader in adopting mobile and wireless technology, perhaps because of the frequent urgency of communications with doctors and nurses, who are almost always on the move. For example, doctors were among the first large groups to start using personal digital assistants

(PDAs) on the job. Other common uses of wireless technology in the healthcare field include the following:

- Providing a means to access and update EHRs at patients' bedsides to ensure accurate and current patient data
- Enabling nurses to scan bar codes on patient wristbands and on medications to help them administer the right drug in the proper dosage at the correct time of day (an attached computer on a nearby cart is linked via a wireless network to a database containing physician medication orders)
- Using wireless devices to communicate with healthcare employees wherever they may be

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, laptop and tablet computers, videoconferencing, streaming media, and store-and-forward, high-resolution imaging are technologies frequently used to support telehealth.

Thousands of mobile applications are available to improve patient access to healthcare information and to enable doctors to keep a close watch on patients' conditions. Appointment and prescription reminders, medication and vital sign tracking, and diet and weight monitoring are common applications based on the sending of text messages to the patient, the healthcare professional, or 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.[65]

There are potential issues with the use of mobile applications, 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. HIPAA regulations could be violated if sensitive patient information is sent via standard text messages. This ruling is driving developers of mobile apps to move away from the use of SMS text messages to a more secure communications method.[66]

Telemedicine is the component of telehealth that provides medical care to people at a location different from the healthcare providers. This technology reduces the need for patients to travel for treatment and allows healthcare professionals to serve more patients in a broader geographic area. 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 (see Figure 8-6). This type of monitoring does not require the presence of the patient and care provider at the same time. Yet, having access to such information can enable healthcare professionals to recognize problems and intervene with remote patients before high-risk situations become life threatening.

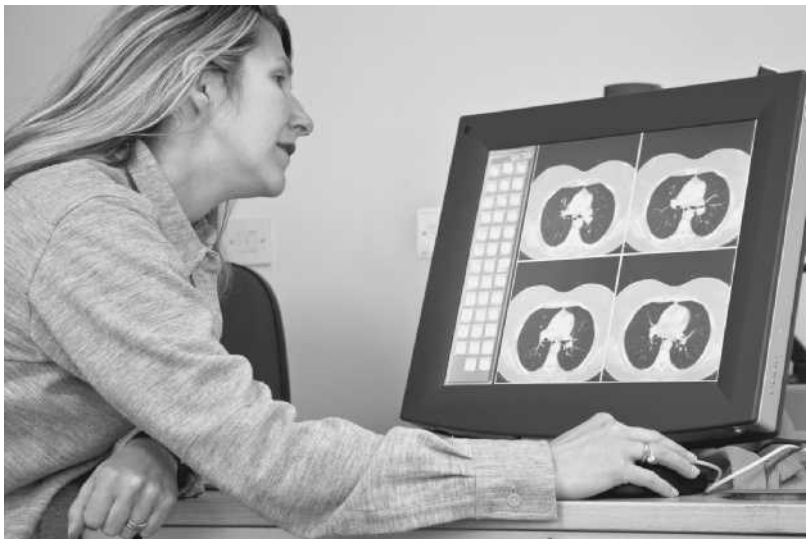


FIGURE 8-6 Teleradiology involves the transfer of CT scans, MRIs, X-rays, and other forms of medical imaging—such as to an imaging center for review by a radiologist
Credit: © iStockphoto.com/WILLSIE.

In one example, the life of a 16-year-old Venezuelan boy was saved by the use of store-and-forward telemedicine. He was admitted to a rural clinic in Venezuela with severe abdominal pain and a large abdominal mass. The local physician examined the boy and sent his findings via the Internet to a specialty physician hundreds of miles away. The specialist recognized a potential deadly condition and requested emergency surgery be performed immediately.[67]

Live telemedicine requires the presence of patients and healthcare providers at different sites at the same time and often involves a videoconference link between the two sites. For example, work on an oil rig can be extremely dangerous and the nearest hospital is often hundreds of miles away. Oil companies are increasingly relying on live telemedicine to connect a nurse or EMT on an oil platform to emergency physicians at a major medical center.

Remote monitoring (also called home monitoring) involves the regular, ongoing 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. Patients who have chronic diseases often don't recognize early warning signs that indicate an impending health crisis. For example, a sudden weight gain by a patient who has suffered congestive heart failure could indicate retention of fluids, which could lead to a traumatic trip to the emergency room or even loss of life. While the patient might not be aware of the potential danger, a physician using telemedicine to keep tabs on such a patient could be alerted to this potentially life-threatening development before a health crisis occurs. It is estimated that 2.8 million people worldwide used some form of home monitoring device in 2012.[68]

The use of telemedicine does raise some new 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 videoconferencing 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 crisis 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 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.[69]

Medical Information Web Sites for Laypeople

Healthy people as well as those who suffer from illness need reliable information on a wide range of medical topics to learn more about healthcare services and to take more responsibility for their health. Clearly, laypeople cannot become as informed as trained medical practitioners, but a tremendous amount of healthcare information is available via the Web. These sites have a critical responsibility to publish current, reliable, and objective information. Table 8-5 provides just a small sample of Web sites that offer information on a variety of medical-related topics.

The contents of a medical information Web site, such as text, graphics, and images, are for informational purposes only. These Web sites are not intended to be substitutes for professional medical advice, diagnosis, or treatment. Individuals should always seek the advice of a physician or other qualified healthcare provider with any questions regarding a medical condition. A patient should never disregard professional medical advice or delay seeking it because of something he or she reads on a medical information Web site.

In addition to publicly available information on the Web, many healthcare providers, employers, and medical insurers offer useful online tools that go beyond basic health information. These tools enable patients to go online and compare the quality, safety, and cost information on hospitals nationwide. You can also find risk indicators for specific health treatment options and nationwide average prices of drugs and treatment options. In addition, the coverage and costs for treatments by in-network and out-of-network healthcare providers can be found on many of these Web sites.

For example, an individual who needs a hip replacement can go online and find information about the surgery; other available treatment options; a list of questions to ask the physician; potential risks; nearby hospitals that perform the surgery; and quality-of-service information about the hospitals, such as the number of reported postoperative infections and other complications.

TABLE 8-5 Health information Web sites

URL	Site
www.americanheart.org	American Heart Association
www.cancer.org	American Cancer Society
www.cdc.gov	Centers for Disease Control and Prevention
www.diabetes.org	American Diabetes Association
www.healthcentral.com	A collection of Web sites that includes news and videos on health topics
www.heartburn.about.com	Information on the causes of heartburn and how to prevent it
www.heartdisease.about.com	Basic information about heart disease and cardiology
www.medicinenet.com	Source for medical information on a variety of topics, including symptoms, procedures, tests, and medications, as well as a medical dictionary
www.mentalhelp.net	A site that promotes mental health and wellness plus education
www.nia.nih.gov/Alzheimers	National Institute on Aging—Alzheimer's Disease Education and Referral Center
www.niddk.nih.gov	National Institute of Diabetes and Digestive and Kidney Diseases
www.oncolink.org	Abramson Cancer Center of the University of Pennsylvania
www.osteo.org	National Institutes of Health—Osteoporosis and Related Bone Diseases National Resource Center
www.urologyhealth.org	Information about urologic conditions, including erectile dysfunction, HIV, AIDS, kidney stones, and STDs
www.webmd.com	Access to medical reference material and online professional publications

Source Line: Course Technology/Cengage Learning.

Summary

- 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.
- Productivity is defined as the amount of output produced per unit of input.
- Most countries have been able to produce more goods and services over time—not through a proportional increase in input but 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.
- Progressive management teams 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.
- Telework (also known as telecommuting) is a work arrangement in which an employee works away from the office—at home, at a client's office, in a hotel—literally, anywhere.
- Many organizations offer telework opportunities to their employees as a means of reducing costs, improving morale, reducing turnover, increasing productivity, reducing the organization's carbon footprint, and allowing for the continuity of business operations.
- Telework opportunities provide many advantages for employees, such as avoiding long, stressful commutes, providing more flexibility to balance the needs of work and family life, and enabling people with disabilities to be productive members of the workforce.
- The *digital divide* is a term used to describe the gulf between those who do and those who don't have access to modern information and technology, such as smartphones, personal computers, and the Internet.
- The digital divide exists not only between more and less developed countries but also within countries—among age groups, economic classes, and people who live in cities versus those in rural areas.
- The Education Rate (E-Rate) program was created through the Telecommunications Act of 1996. The E-Rate program helps schools and libraries obtain broadband Internet services to advance the availability of educational and informational resources.
- One Laptop per Child is a nonprofit organization whose goal is to provide children around the world with low-cost laptop computers to aid in their education. Intel and the Raspberry Pi Foundation also provide low-cost computers for educational purposes.
- Many people think that it will be the cell phone and the smartphone—and not the computer—that will ultimately bridge the digital divide.
- Healthcare costs are soaring and are expected to increase an average of 6.3 percent per year from 2015 to 2021.

- To gain control over healthcare costs, patients will need to gain a much greater awareness of medical costs, and new technology costs will need to be managed more carefully.
- Improved use of IT in the healthcare industry can lead to significantly reduced costs in a number of ways: Electronic health records (EHRs) of patient information can be generated from each patient visit in every healthcare setting; wireless technology can be used to access and update EHRs at patients' bedsides, match bar-coded patient wristbands and medication packages to physician orders, and communicate with healthcare employees wherever they may be.
- Skeptics question the ability of EHR to lower healthcare costs and improve the quality of care.
- 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. It reduces the need for patients to travel for treatment and allows healthcare professionals to serve more patients in a broader geographic area.
- Web-based health information can help people inform themselves about medical topics.

Key Terms

digital divide
Education Rate (E-Rate) program
electronic health record (EHR)
Health Information Technology for Economic and Clinical Health Act (HITECH Act)
live telemedicine
One Laptop per Child (OLPC)
productivity
remote monitoring
store-and-forward telemedicine
telehealth
telemedicine
telework

Self-Assessment Questions

The answers to the Self-Assessment Questions can be found in Appendix B.

1. Which of the following statements about the standard of living is *not* true?
   a. It is frequently measured using the gross domestic product per capita.
   b. It varies little among groups within the same country.
   c. Industrialized nations generally have a higher standard of living than developing countries.
   d. It varies greatly from nation to nation.
2. _____ is the amount of output produced per unit of input.
3. The period of time with the highest level of nonfarm productivity in the United States is _____.
   a. 1947–1973
   b. 1973–1979
   c. 2000–2007
   d. 2007–2012

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. over seven years to fully recover the initial investment costs.
   d. five to seven years to result in a substantial increase in productivity.
5. _____ is a term used to describe the gulf between those who do and those who don't have access to modern information and communications technology, such as cell phones, smartphones, personal computers, and the Internet.
6. It is estimated that during 2011, roughly _____ of employed Americans worked at least one day per week from home.
   a. 0% to 10%
   b. 10% to 20%
   c. 20% to 30%
   d. 30% to 40%
7. The group(s) of people living in the United States that is least likely to have Internet access is/are _____.
   a. Hispanics and African Americans
   b. urban dwellers
   c. residents of the Northeast
   d. Asians
8. North America has a greater Internet penetration rate than Asia. True or False?
9. The _____ program was designed to eliminate the digital divide in the United States by helping schools and libraries obtain high-speed Internet connections.
10. Which of the following statements about healthcare spending is *not* true?
    a. U.S. spending on health care in 2011 was about $2.7 trillion.
    b. The development and use of new medical technology in the United States has clearly led to a reduction in healthcare costs.
    c. Much of the growth in healthcare costs is due to the continued aging of the population in the United States.
    d. U.S. spending on health care is expected to increase an average of 6.3 percent from 2015 until 2021.
11. Some studies have estimated that at least 98,000 people die in hospitals each year due to preventable mistakes. True or False?
12. A(n) _____ is a summary of health information generated by each patient encounter in any healthcare delivery setting.
13. Under the Health Information Technology for Economic and Clinical Health Act, increased Medicaid or Medicare reimbursements will be made to doctors and hospitals that demonstrate _____ of EHR technology.

Discussion Questions

1. Discuss how the average annual percent change in nonfarm productivity has varied over the past 65 years.
2. Briefly discuss the correlation between IT investment and U.S. productivity growth.
3. Why is it harder to quantify the benefits of today's IT investments than it was in the 1960s?
4. Define the term telework. What technologies are essential for effective telework?
5. Would you accept a telework position in which you would work from home three or four days per week? Why or why not?
6. What is the digital divide? Where does it exist? Why is it important to bridge the digital divide?
7. What is your opinion of the effectiveness of the E-Rate program? What facts back up your opinion?
8. Which tool do you believe can be most effective in bridging the digital divide—the personal computer or the smartphone? Why?
9. 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? Which approach to dealing with moral issues discussed in Chapter 1 would you use to analyze this question? What decision did you come to as a result of your analysis?
10. 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?
11. Medical information that you obtain from Web sites must be accurate and reliable. Identify three characteristics of a credible Web site.

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. It is the year 2028, and robots are being introduced to handle the screening of patients at physicians' offices in the United States. The robots look human 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 then 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, and college campuses. The goal of using 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 would you do to make the use of a robotic physician assistant more acceptable to patients and to ensure patient care does not suffer?

2. You have been diagnosed with a rare bone marrow disorder that affects only 2 people out of 1 million. The disease is potentially life threatening, but your symptoms are currently only mild and do not yet present a major concern. Your physician recommends that you go to the Mayo Clinic in Rochester, Minnesota, for further diagnosis and possible treatment. As you do some research on the Internet, you find a support group for those afflicted by this rare disease. You are alarmed to hear that the disease can cause a very rapid decrease in the quality of one's life, with many victims confined to a wheelchair or bed and in great discomfort for the last months of their life. When you meet with specialists at the Mayo Clinic, they provide a much more optimistic outlook and claim that medical breakthroughs in treating the disease have been made. You do not know what to believe. You wonder about reaching out to the support group to get further information or to convey what doctors have told you. What would you do?
3. You are in your local computer store and see a "low-cost" laptop selling for just $299. There is a note on the price tag stating that $50 of the purchase price will be used to subsidize the cost of this computer to students in developing countries. How do you feel about paying an extra $50 for this purpose? Would you attempt to negotiate a lower price? Would you be willing to pay the additional $50?
4. 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 in 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?
5. As a second-year teacher at a low-rated inner-city elementary school, you have been asked to form and lead a three-person committee to define and obtain funding for an E-Rate program for your school. Do some research on the Internet and outline a process you would follow to request funding.
6. You are a recent college graduate and an employee of a high-tech firm located in Silicon Valley. In a highly unusual move, your company's Human Resources Department is conducting a series of focus groups to get employee input on a number of issues, including telework. You have been invited to attend one of the focus group sessions and have been asked to be prepared to discuss your feelings on the firm's current telework policy. The current policy is that telework is not approved for employees unless they will be out of the

office for an extended period of time due to illness. You will be given two minutes to express your opinion. What would you say?

7. You are an elected official in a small, third-world country's house of parliament, which is responsible for initiating revenue spending bills. Your country is very poor; unemployment is high; most families cannot afford a healthy diet; there is an insufficient amount of doctors and healthcare services; and there is an inadequate infrastructure for water, telephone, and power. Recently, senior executives from technology firms have approached you and lobbied you strongly to support increased spending on information technology infrastructure, including the placement of 1 million low-cost computers in your nation's schools. They make a strong case that the computers will increase the educational opportunities for your nation's children. They are willing to subsidize one-half of the estimated $1 billion (USD) required to implement this program successfully. While their idea provides hope for a better life for the children, your country has many needs. How would you proceed to evaluate this opportunity and weigh its costs against your country's other needs?
8. You have volunteered to lead a group of citizens in approaching the board of directors of the nearest hospital (55 miles away) about establishing remote monitoring of 50 or so chronically ill people in your small community. What sort of facts do you need to gather to make a sound recommendation to the board? What are some specific items that you would request?
9. You have been offered a position as a software support analyst. If you accept, you will have three weeks of on-site training, after which you will work from your home full-time, answering customer service calls. What questions would you want answered before you decide whether or not to take this position?

Cases

1. Is the Tide Turning on Telework?

Tech companies in Silicon Valley are often noted for their generous employee benefits, such as providing free meals for workers, allowing dog owners to bring their pets to work, and offering flexible working hours, including support for telework from home. The goal of these policies is to encourage workers to put in longer hours at work or to work more productively. Thus, it came as a surprise when Marissa Mayer, newly appointed CEO of Yahoo!, directed her human resources chief to send out a memo to all employees that essentially put an end to flexible work hours and the ability of Yahoo! employees to work from home. The memo said in part: "Speed and quality are often sacrificed when we work from home. We need to be one Yahoo!, and that starts with physically being together." Yahoo!'s move is an attempt to improve collaboration and to become more competitive.[70,71]

The change in policy came at a difficult time for Yahoo!. The firm went through four CEOs in five years, and industry experts had been questioning Yahoo!'s ability to develop new and innovative services. Many have also questioned the quality of its workforce.[72] After Yahoo!'s earnings were announced on April 17, 2013, shares in the company fell more than 3 percent on news of a decrease in sales of display ads.[73]

The ban on working from home drew both sharp criticism and praise from industry observers and employees. On the negative side, management consultants and authors Jody Thompson and Cali Ressler believe the policy change is a major mistake and that Yahoo! will end up with workers who earn good work attendance marks but are not effective and efficient at meeting company goals.[74] Jennifer Glass—a sociology professor and research associate at the Population Research Center at the University of Texas, Austin—points out that the United States already trails other industrialized nations when it comes to providing flexible work arrangements. Sir Richard Branson, billionaire business magnate and founder of Virgin Airlines and Virgin Records, said Mayer's policy was a step backwards "in an age when remote working is easier and more effective than ever." Another professor felt that the changed policy could further lower employee morale and hurt recruiting efforts.[75]

Supporters of the new policy include many who believe that employees are more productive in the office. Just prior to Yahoo!'s announcement, Patrick Pichette, CFO at Yahoo! rival Google, had pointed out that his firm believes strongly in employees working physically close to one another to encourage collaboration.[76] Perhaps encouraged by Mayer's announcement, just one week after Yahoo!'s change in policy, Best Buy informed its headquarters employees that its flexible work program was canceled and that it expected employees to work a traditional 40-hour week at its headquarters. The need to collaborate and work together in turning the company around was given as the reason for the change in policy.[77]

Discussion Questions

1. Do further research on business results and employee morale at Yahoo! to develop an opinion on whether the ban on telework has helped the firm. Write a paragraph stating your opinion and providing supporting facts.
2. Should telework only be considered a "perk" for those companies and employees that are already producing good business results? Why or why not?
3. Imagine that you are a member of a firm's human resources group trying to decide whether or not to support telework. What factors would you consider in making this decision? What process would you follow to arrive at a decision that could be accepted by employees and senior management as well?

2. Kaiser Permanente Implements Electronic Health Record (EHR) System

Kaiser Permanente is an integrated healthcare organization founded in 1945. The company operates one of the nation's largest not-for-profit health plans, with over 9 million health plan subscribers. Kaiser Permanente also includes Kaiser Foundation Hospitals (encompassing 37 hospitals) and The Permanente Medical Groups, with 611 medical offices. The company employs nearly 173,000 people, including 16,658 physicians. Its 2011 operating revenue was almost $48 billion.[78]

HealthConnect is the name of Kaiser's comprehensive health information system, which includes an EHR application that was fully implemented at all of its hospitals and clinics in March 2010. In 2003, Kaiser had announced its intention to work with Epic Systems Corporation over a three-year period to build an integrated set of systems to support EHRs, computerized physician order entry, scheduling and billing, and clinical decision support at an estimated cost of $1.8 billion. This decision came after Kaiser had already made several unsuccessful attempts

at clinical automation projects. The project eventually ballooned into a seven-year, $4.2 billion effort as the scope of the project was expanded time and again.[79] Training and productivity losses made up more than 50 percent of the cost of the project as Kaiser had to cut physicians' hours at clinics during training and was forced to hire physicians temporarily to handle the workload.[80]

The HealthConnect system connects Kaiser plan subscribers to their healthcare providers and to their personal healthcare information. The system uses EHRs to coordinate patient care among physician's offices, hospitals, testing labs, and pharmacies. The EHR is designed to ensure that patients and their healthcare providers all have access to current, accurate, and complete patient data. The system and its data are now accessible via smartphone as well as personal computer. During 2012, there were over 88 million subscriber sign-ons to the system.[81]

Physicians and nurses in hospitals, clinics, and private offices document treatment in the EHR system. After a physician enters a diagnosis into the system, he or she may receive a system message indicating that there is a "best practice order set" available for treating the condition. When they enter a medication order, physicians receive alerts about potential allergic reactions or adverse drug reactions based on other medications a patient is already taking.[82] Physicians also receive automatic notifications about how lab test results should affect medication orders.[83]

HealthConnect also provides capabilities to support bar coding for the safe administration of medicine. Under this system of administering medication, the nurse first scans the patient's barcoded identification wristband. The nurse next scans a bar code on the medication container that identifies the specific medicine and dosage. The system verifies that this medicine and dosage has been ordered for this patient. If there is not a match, the nurse receives an audible warning signal.[84]

Kaiser has found that use of a comprehensive EHR improves health plan subscribers' satisfaction with the healthcare delivery system. In addition, HealthConnect empowers healthcare plan subscribers to take more responsibility for managing their own health care. Kaiser subscribers can access HealthConnect via a Web portal at *kp.org.* Here they are able to view most of their personal health records online, including their lab results, medication history, and treatment summaries. Patients can enter their own readings from blood pressure and glucose meters.[85] They can also securely email their healthcare providers, which cuts down on the amount of time patients spend on hold waiting to speak to a doctor and on the number of office visits (the number of outpatient visits has dropped an average of 8 percent in the one and one-half years following EHR implementation at each hospital).[86] Each month patients send over 1 million emails to their doctors and healthcare teams through this component of the system. Over 29 million lab test results were viewed online in 2011. In addition, approximately 827,000 prescriptions are being refilled online monthly, and 230,000 appointments are scheduled monthly.[87]

HealthConnect enables physicians to benchmark their performance against colleagues on a number of fronts—efficiency, quality, safety, and service. Hospitals can also benchmark each other on measures such as adverse events and complications. "Best in class" practices can be identified, and physicians and hospitals can borrow these best practices from one another to further improve the overall quality of care.[88]

Kaiser began working on implementing an EHR system in 2003 and finally completed the implementation in 2010. Along the way, the company tried several different approaches, ran into numerous problems, and spent millions of dollars. It is just now beginning to reap the benefits

from this effort. It likely will take time, further system enhancements, and additional expenditures for many other organizations to see similar benefits.

Discussion Questions

1. What do you think are the greatest benefits of the HealthConnect system for Kaiser Permanente subscribers? Can you identify any potential risks or ethical issues associated with the use of this system for Kaiser healthcare plan subscribers? How would you answer these questions from the perspective of a physician or nurse?
2. This system took over seven years to implement and is estimated to have cost at least $4.2 billion. Would you say that this was a wise investment of resources for Kaiser Permanente? Why or why not?
3. Researchers associated with Kaiser Permanente have used the patient record database to make numerous worthwhile discoveries in the areas of preventing whooping cough, determining the correlation between HPV vaccination and sexual activity in young girls, improving methods of cancer detection, avoiding blood clots in women using birth control pills, and lowering cholesterol. Do you think that access to this valuable data should be granted to researchers not associated with Kaiser Permanente? What potential legal and ethical issues could arise if this were done? Should researchers be charged a fee to access this data to help offset the ongoing cost of upgrading the system?

3. Decision Support for Healthcare Diagnosis

Diagnosis errors (including missed, wrong, or delayed diagnosis) are a frequent and serious problem in the healthcare industry. It is estimated that such errors result in death or permanent injury for up to 160,000 U.S. patients each year. In a recent Johns Hopkins University study examining malpractice claims, researchers found that claim payments for diagnostic errors added up to $38.8 billion over the time period 1986 to 2010.[89] Failure to fully diagnose a patient's condition puts the patient at risk of suffering a recurrence of the problem—such as incurring further damage from another accident caused by, for example, an undiagnosed brain injury. Misdiagnosis of a patient's condition can lead to costly, painful, potentially harmful, and inappropriate treatments. A delay in the diagnosis of a patient can allow an otherwise reversible condition to advance to the point that it is no longer treatable.

Over the past decade, several decision support systems to aid in healthcare diagnosis have been developed, including DiagnosisPro®, DXPlain®, First Consult©, PEPID, and Isabel©. A decision support system is an interactive computer application that aids in decision making by gathering data from a wide range of sources and presenting that data in a way that aids in decision making. Isabel, one of the more advanced healthcare decision support systems, is a Web-based system developed in the United Kingdom. Isabel uses key facts from the patient's history, physical exam, and laboratory findings to identify the most likely diagnosis based on pattern matches in the system's database. The system can interface with electronic medical records systems to obtain patient data, or the data can be entered manually. Each diagnosis is linked to information in commonly used medical reference sources such as *The 5 Minute Clinical Consult, Oxford Textbook of Medicine,* and Medline—the U.S. National Laboratory of Medicine's online bibliographic database. Isabel can also suggest bioterrorism agents that might be responsible for a patient's symptoms, as well as identify drugs or drug combinations

that might be the cause.[90] The cost of using Isabel ranges from a few thousand dollars for a family practice to as much as $400,000 for a health system.[91]

United Hospital, a large hospital in St. Paul, Minnesota, recently implemented the Isabel system to help physicians investigate and diagnose patient cases. The system will integrate directly with the hospital's electronic medical record system and physicians will be able to access Isabel from mobile devices.[92]

On another front, medical researchers at Memorial Sloan-Kettering Cancer Center in New York are busy feeding data from medical textbooks and journals into IBM's Watson supercomputer to create a world-class healthcare diagnostic tool. Watson is the same supercomputer that gained recognition in 2011 for beating the world's best players on the TV game show *Jeopardy!*. Watson is now being programmed to understand plain language so that it can absorb data about a patient's symptoms and medical history, form a diagnosis, and suggest an appropriate course of treatment. When presented with a set of symptoms, Watson will be able to provide several diagnoses, ranked in order of its confidence.[93,94]

One incentive hospitals have to adopt such systems is concern that a failure to adopt new technology could subject the hospital to liability in cases where it could be shown that adoption of the technology would not have been overly costly and could have prevented patient injury.[95]

Discussion Questions

1. What concerns might a physician have about using a decision support system such as Isabel or Watson to make a medical diagnosis? How might those concerns be alleviated?
2. Is it possible that in a decade this type of technology could be easily accessible by laypeople who could then perform self-diagnosis, thus helping to reduce the cost of medical care?
3. Does the use of decision support systems to support healthcare decisions seem like an effective way to reduce healthcare costs? Why or why not?

End Notes

1 Edward Wyatt, "Fund That Subsidizes Internet for Schools Should Expand, a Senator Says," *New York Times*, March 12, 2013, www.nytimes.com/2013/03/13/technology/fund-that-subsidizes-internet-for-schools-should-expand-a-senator-says.html?_r=1&.

2 Education and Library Networks Coalition, "Get the Facts," www.edlinc.org/get_facts.html#Is the E-Rate program working (accessed April 6, 2013).

3 Edward Wyatt, "Fund That Subsidizes Internet for Schools Should Expand, a Senator Says," *New York Times*, March 12, 2013, www.nytimes.com/2013/03/13/technology/fund-that-subsidizes-internet-for-schools-should-expand-a-senator-says.html?_r=1&.

4 The Associated Press, "Illinois Woman Gets Prison for School Bribery Plot," *Times Picayune*, February 9, 2012, www.nola.com/education/index.ssf/2012/02/illinois_woman_gets_prison_for.html.

5 Funds for Learning, "FCC and Department of Justice Investigate E-Rate Fraud," February 15, 2012, www.fundsforlearning.com/news/2012/02/fcc-and-department-justice-investigate-e-rate-fraud.

[6] USAC, "Suspensions & Disbarments," www.usac.org/sl/about/program-integrity/suspensions-debarments.aspx (accessed May 1, 2013).

[7] Marguerite Reardon, "Eroding E-Rate," *CNET*, June 17, 2004, http://news.cnet.com/Eroding-E-rate/2009-1028_3-5236723.html.

[8] Robert Wilonsky, "DOJ, FCC Settle with HP (for $16.25 Mil!) Over E-Rate Fraud in Dallas, Houston ISDs," *Crime* (blog), *Dallas Observer*, November 10, 2010, http://blogs.dallasobserver.com/unfairpark/2010/11/doj_fcc_settle_with_hp_for_162.php.

[9] Lynn Walsh, "Gift-Giving Culture Flourished at HISD; Vendors Lavished Cash, Dinners and Tickets on Employees," July 20, 2010, www.texaswatchdog.org/taxonomy/term/143; and Lynn Walsh, "Hewlett-Packard to Pay $16M+ as More Problems Come Out in HISD, DISD E-Rate Program," *Texas Watchdog*, November 11, 2010, www.texaswatchdog.org/2010/11/erate/1289514507.column.

[10] Grant Gross, "Dallas School District Settles E-Rate Fraud Case," *CIO*, June 26, 2009, www.cio.com/article/496107/Dallas_School_District_Settles_E_Rate_Fraud_Case.

[11] "Whistleblower Realtors Dan Cain, Pamela Tingley, Dave Richardson & Dave Gillis Win HP E-Rate Program Settlement," Outlook Series, November 11, 2010, www.outlookseries.com/A0999/Financial/3801_Whistleblower_Relators_Dan_Cain_Pamela_Tingley_Dave_Richardson_Dave_Gillis_Win_HP_E-Rate_Program_Settlement.htm.

[12] GAO-10-908, "FCC Should Assess the Design of the E-Rate Program's Internal Control Structure," The General Accounting Office, September 2010, www.gao.gov/assets/320/310686.pdf.

[13] E-Rate Central's Guide to Preparing for and Surviving E-Rate Audits," E-RateCentral.com, www.e-ratecentral.com/applicationTips/ten_audit_tips.pdf.

[14] Funds for Learning, "GAO: 'Overall Design of E-Rate Is Complex,'" November 2, 2010, www.fundsforlearning.com/news/2010/11/gao-overall-design-e-rate-complex.

[15] Funds for Learning, "USAC Seeks Independent Auditor for E-Rate Risk Assessment," October 11, 2012, www.fundsforlearning.com/news/2012/10/usac-seeks-independent-auditor-e-rate-risk-assessment.

[16] Kimberly Amadeo, "The Great Depression of 1929," *About.com*, www.about.com/od/grossdomesticproduct/p/1929_Depression.htm.

[17] Kimberly Amadeo, "GDP 2008 Statistics," *US Economy*, April 30, 2011, http://useconomy.about.com/od/GDP-by-Year/a/2008-GDP-statistics.htm.

[18] Peter S. Goodman, "Unemployment Rate Hits 10.2%, Highest in 26 Years," *New York Times*, November 6, 2009.

[19] Stephen D. Oliner and William L. Wascher, "Is a Productivity Revolution Underway in the United States?," *Challenge*, November-December 1995, www.questia.com/googleScholar.qst;jsessionid=K2sGFsv9Dtjpghh25XQYNGcZcWNVv4hGWLJJ1sLX0wJtGGX2RZZq!1481560549!1622387428?docId=5000361656.

[20] U.S. 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).

[21] Erik Brynjolfsson and Lorin M. Hitt, "Computing Productivity: Firm-Level Evidence," November 2002, http://opim.wharton.upenn.edu/~lhitt/cpg.pdf.

[22] U.S. Bureau of Labor Statistics, "News Release: American Time Survey—2011 Results," June 22, 2011, www.bls.gov/news.release/pdf/atus.pdf.

[23] Global Workplace Analytics, "Latest Telecommuting Statistics," www.globalworkplaceanalytics.com/telecommuting-statistics (accessed April 21, 2013).

[24] Andrew Ujifusa, "Telecommuting Remains Rare Among State Employees," *Gazette.net*, January 6, 2012, www.gazette.net/article/20120106/NEWS/701069664/-1/telecommuting-remains-rare-among-state-employees&template=gazette.

[25] Amanda Palleschi, "More Than 20 Percent of Employees Now Telework, OPM Says," *Government Executive*, July 6, 2012, www.govexec.com/technology/2012/07/opm-releases-its-most-comprehensive-report-telework-practices/56669.

[26] Andrew Dunn, "Bank of America Is Cutting Back on At-Home Workers," *Banking*, December 5, 2012, www.charlotteobserver.com/2012/12/05/3706260/bank-of-america-at-home-work.html.

[27] "Best Buy Copies Yahoo, Reins in Telecommuting," *USA Today*, March 6, 2013, www.usatoday.com/story/money/business/2013/03/06/best-buy-telecommuting-ban-yahoo/1966667.

[28] Rick Hampson, "Yahoo's Ban on Telecommuting Brings Up Question—Who Benefits?," *AZCentral.com*, March 11, 2013, www.azcentral.com/news/articles/20130311yahoo-ban-telecommuting-brings-question-who-benefits.html.

[29] "The Impact of Teleworking—The Views of Teleworkers," Australian Government Department of Communications, Information Technology and the Arts, February 5, 2008, www.archive.dcita.gov.au/2007/11/australian_telework_advisory_committee/sensis_insights_report_teleworking/the_impact_of_teleworking__the_views_of_businesses.

[30] Mary C. Noonan and Jennifer L. Glass, "The Hard Truth About Telecommuting," *Monthly Labor Review*, June 2012, www.bls.gov/opub/mlr/2012/06/art3full.pdf.

[31] Subba Rao NV, "Digital Divide in India," *reboot* (blog), December 28, 2012, http://reboot.co.in/blog/digital-divide-in-india.

[32] Kathryn Zickuhr and Aaron Smith, "Pew Internet Digital Differences," Pew Internet & American Life Project, April 13, 2012, www.pewinternet.org/Reports/2012/Digital-differences/Overview.aspx.

[33] Antone Gonsalves, "Study: Internet Has No Impact on Student Performance," *InformationWeek*, November 21, 2005.

[34] Internet World Stats, "World Internet Usage and Population Statistics," June 30, 2012, www.internetworldstats.com/stats.htm.

[35] Mika Turim-Nygren, "Can Tech Really Transform the Third World? A One Laptop Per Child Report Card," *Digital Trends*, February 20, 2013, www.digitaltrends.com/computing/from-australia-to-africa-olpc-gives-students-a-window-on-the-world.

[36] Edgar Alvarez, "OLPC X0-4 to Sell Starting at $206, Production Commencing March," *engadget*, January 8, 2013, www.engadget.com/2013/01/08/olpc-xo-4-pricing.

[37] Mika Turim-Nygren, "Can Tech Really Transform the Third World? A One Laptop Per Child Report Card," *Digital Trends*, February 20, 2013, www.digitaltrends.com/computing/from-australia-to-africa-olpc-gives-students-a-window-on-the-world/.

[38] "Nepal," Foundation Nepal, www.foundation-nepal.org/content/nepal (accessed April 23, 2013).

[39] "Nepal Unemployment," Index Mundi, www.indexmundi.com/nepal/unemployment_rate.html (accessed April 23, 2013).

[40] OLPC, "Open Learning Exchange Nepal Enters Into Its Fourth Year," May 23, 2011, www.olpcnews.com/countries/nepal/open_learning_exchange_nepal_e.html.

[41] Michael Kanellos, "Intel's Bridge for the Digital Divide, *CNET*, June 15, 2006, http://news.cnet.com/Intels-bridge-for-the-digital-divide/2100-1005_3-6084250.html.

[42] Intel Corporation, "Product Brief: The Classmate PC Powered by Intel," www.intel.com/content/dam/doc/product-brief/data-center-efficiency-xeon-5600-cisco-united-computing-system-brief.pdf (accessed May 28, 2013).

[43] "Intel: 4 Million Classmate PC Netbooks Deployed," *liliputing* (blog), June 23, 2011, http://liliputing.com/2011/06/intel-4-million-classmate-pc-netbooks-deployed.html.

[44] Intel, "Intel-Powered Convertible Classmate PC: Netbooks Designed for Learning and Collaboration," www.intel.com/content/www/us/en/education-solutions/netbooks-for-learning-brief.html (accessed April 23, 2013).

[45] Raspberry Pi, "About Us," www.raspberrypi.org/about (accessed May 28, 2013).

[46] Patrick Thibodeau, "Different and Cheap, New $25 Raspberry Pi Is Selling," *Computerworld*, April 3, 2013, www.computerworld.com/s/article/9238082/Different_and_cheap_new_25_Raspberry_Pi_is_selling.

[47] Centers for Medicare and Medicaid Services, "National Health Expenditure Projections 2011–2021," www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/Proj2011PDF.pdf (accessed April 23, 2013).

[48] Jason Fodeman, M.D. and Robert A. Book, PhD, "Bending the Curve: What Really Drives Healthcare Spending," The Heritage Foundation, February 17, 2010, www.heritage.org/Research/Reports/2010/02/Bending-the-Curve-What-Really-Drives-Health-Care-Spending.

[49] Parjia Kavilanz, "6 Reasons Health Care Costs Keep Going Up," *CNN Money*, July 12, 2012, http://money.cnn.com/2012/07/12/news/economy/health-care-costs/index.htm.

[50] 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.

[51] Rebecca Adams, "Washington Health Policy Week in Review Health IT Investments Will Top Industry Concerns in 2011," The Commonwealth Fund, December 20, 2010, www.commonwealthfund.org/Content/Newsletters/Washington-Health-Policy-in-Review/2010/Dec/December-27-2010/Health-IT-Investments-Will-Top-Industry-Concerns-in-2011.aspx.

[52] Knapp & Roberts, "Press Release: Preventable Medical Mistakes: A National Nightmare," *24-7 Press Release*, January 6, 2010, www.24-7pressrelease.com/press-release/preventable-medical-mistakes-a-national-nightmare-131199.php.

[53] "HITECH Act: The Health Information Technology for Economic and Clinical Health (HITECH) Act, ARRA Components," January 6, 2009, HITECH Survival Guide, www.hipaasurvivalguide.com/hitech-act-text.php.

[54] Dustin Charles, MPH; Jennifer King, PhD; Vaishali Patel, PhD; and Michael F. Furukawa, PhD, "Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2012," Office of the National Coordinator for Health Information Technology, March 2013, www.healthit.gov/sites/default/files/oncdatabrief9final.pdf.

[55] "EHR Adoption Rate in US Hospitals to Rise Through 2014?," *InfoGrok Healthcare*, April 16, 2010, www.infogrok.com/index.php/prediction-healthcare/ehr-adoption-rate-in-us-hospitals-to-rise-through-2012.html.

[56] "HITECH Act: The Health Information Technology for Economic and Clinical Health (HITECH) Act, ARRA Components, January 6, 2009, HITECH Survival Guide, www.hipaasurvivalguide.com/hitech-act-text.php.

[57] "RAND Study Says Computerizing Medical Records Could Save $81 Billion Annually and Improve the Quality of Medical Care," RAND Corporation, September 14, 2005, www.rand.org/news/press/2005/09/14.html.

[58] Cheryl Clark, "EHR Effectiveness for Hospital Care Questioned," *Health Leaders Media*, December 29, 2010, www.healthleadersmedia.com/content/TEC-260743/EHR-Effectiveness-for-Hospital-Care-Questioned.

[59] Glen Tullman, "Why Haven't Electronic Health Records Made Us Healthier?," *Forbes*, March 13, 2013, www.forbes.com/sites/glentullman/2013/03/04/why-havent-electronic-health-records-made-us-healthier.

[60] Reed Abelson and Julie Creswell, "In Second Look, Few Savings from Digital Health Records," *New York Times*, January 10, 2013, www.nytimes.com/2013/01/11/business/electronic-records-systems-have-not-reduced-health-costs-report-says.html?_r=0.

[61] Lucas Mearian, "Only 10% of Doctors Using Complete e-Health Record Systems, Survey Finds," *Computerworld*, January 18, 2011, www.computerworld.com/s/article/9205238/Only_10_of_doctors_using_complete_e_health_record_systems_surveys_find.

[62] "Rock and a Hard Place: An Analysis of the $36 Billion Impact from Health IT Spending," PricewaterhouseCoopers' Health Research Institute, www.pwc.com/us/en/healthcare/publications/rock-and-a-hard-place.jhtml.

[63] Wake Forest Baptist Medical Center, "About Us," www.wakehealth.edu/News-Media-Resources (accessed May 28, 2013).

[64] Richard Craver, "Wake Forest Baptist Has Cost Overruns, Revenue Loss with Electronic Records System," *Winston-Salem Journal*, April 5, 2013, www.journalnow.com/business/business_news/local/article_c2801866-9e0c-11e2-bf84-0019bb30f31a.html.

[65] 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.

[66] 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.

[67] Telesalud, "Telemedicine Saves Life of Young Pemon from Bolivar State, Venezuela," *International*, www.tele-salud.com/es/node/70 (accessed April 11, 2013).

[68] Carl Weinschenk, "Remote Health Monitoring Will Be Big," *IT Business Edge*, January 23, 2013, www.itbusinessedge.com/blogs/data-and-telecom/remote-health-monitoring-will-be-big.html.

[69] Pauline W. Chen, M.D., "Are Doctors Ready for Virtual Visits?," *New York Times*, January 7, 2010, www.nytimes.com/2010/01/07/health/07chen.html.

[70] Jenna Goudreau, "Back to the Stone Age? New Yahoo CEO Marissa Mayer Bans Working from Home," *Forbes,* February, 25, 2013, www.forbes.com/sites/jennagoudreau/2013/02/25/back-to-the-stone-age-new-yahoo-ceo-marissa-mayer-bans-working-from-home.

[71] Elizabeth Weise and Jon Schwartz, "As Yahoo Ends Telecommuting, Others Say It Has Benefits," *USA Today*, February 26, 2013, www.usatoday.com/story/money/business/2013/02/25/working-at-home-popular/1946575.

[72] Brad Stone, "Marissa Mayer Is Yahoo's New CEO," *Bloomberg Businessweek*, July 16, 2012, www.businessweek.com/articles/2012-07-16/marissa-mayer-is-the-new-yahoo-ceo.

[73] "Yahoo's Q1 Earnings Surge While Revenue Sags," *Times of India*, April 17, 2013, http://timesofindia.indiatimes.com/tech/tech-news/internet/Yahoos-Q1-earnings-surge-while-revenue-sags/articleshow/19587365.cms?.

[74] Elizabeth Weise and Jon Schwartz, "As Yahoo Ends Telecommuting, Others Say It Has Benefits," *USA Today*, February 26, 2013, www.usatoday.com/story/money/business/2013/02/25/working-at-home-popular/1946575.

[75] Jessica Guynn, "Yahoo CEO Causes Uproar with Telecommuting Ban," *Los Angeles Times*, February 26, 2013, http://articles.latimes.com/print/2013/feb/26/business/la-fi-yahoo-telecommuting-20130226.

[76] Ben Grubb, "Do as We Say, Not as We Do: Googlers Don't Telecommute," *Sydney Morning Herald*, www.smh.com.au/it-pro/business-it/do-as-we-say-not-as-we-do-googlers-dont-telecommute-20130219-2eo8w.html#ixzz2TUue1sT5.

[77] Ann Bednarz, "Best Buy Cancels Telework Program," *Network World*, March 5, 2013, www.networkworld.com/news/2013/030513-best-buy-telework-267403.html.

[78] Kaiser Permanente, "About Kaiser Permanente," http://xnet.kp.org/newscenter/aboutkp/fastfacts.html (accessed April 18, 2013).

[79] Neil Versel, "As EHR Installation Nears Completion, Kaiser Recommends 'Big Bang,'" FierceEMR, July 30, 2009, www.fierceemr.com/story/ehr-installation-nears-completion-kaiser-recommends-big-bang/2009-07-30.

[80] Howard J. Anderson, "Kaiser's Long and Winding Road," *Health Data Management*, August 1, 2009, www.healthdatamanagement.com/issues/2009_69/-38718-1.html.

[81] Kaiser Permanente, "Kaiser Permanente HealthConnect® Electronic Health Record," http://xnet.kp.org/newscenter/aboutkp/healthconnect/index.html (accessed April 18, 2013).

[82] Howard J. Anderson, "Kaiser's Long and Winding Road," *Health Data Management*, August 1, 2009, www.healthdatamanagement.com/issues/2009_69/-38718-1.html.

[83] Kaiser Permanente "Kaiser Permanente HealthConnect® Electronic Health Record," http://xnet.kp.org/newscenter/aboutkp/healthconnect/index.html (accessed April 13, 2013).

[84] Kaiser Permanente, "Kaiser Permanente HealthConnect® Electronic Health Record," http://xnet.kp.org/newscenter/aboutkp/healthconnect/index.html (accessed April 18, 2013).

[85] Howard J. Anderson, "Kaiser's Long and Winding Road," *Health Data Management*, August 1, 2009, www.healthdatamanagement.com/issues/2009_69/-38718-1.html.

[86] Howard J. Anderson, "Kaiser's Long and Winding Road," *Health Data Management*, August 1, 2009, www.healthdatamanagement.com/issues/2009_69/-38718-1.html.

[87] Kaiser Permanente, "Kaiser Permanente HealthConnect® Electronic Health Record," http://xnet.kp.org/newscenter/aboutkp/healthconnect/index.html (accessed April 13, 2013).

[88] Jane Sarasohn-Kahn, "The Story of Kaiser Permanente's EHR," *Health Populi*, September 15, 2010, http://healthpopuli.com/2010/09/15/the-story-of-kaiser-permanentes-ehr.

[89] Laura Landro, "Adding Up Diagnosis Errors," *Wall Street Journal*, April 24, 2013, http://online.wsj.com/article/SB10001424127887323551004578438692201899244.html.

[90] Gary Kantor, M.D., "Guest Software Review: Isabel Diagnosis Software," *HISTalk* (blog), January 31, 2006, http://histalk.blog-city.com/guest_software_review_isabel_diagnosis_software_by_gary_kant.htm.

[91] "IBM Jeopardy Winning Watson Computer Delving Into Medicine," *CBS New York*, May 21, 2011, http://newyork.cbslocal.com/2011/05/21/ibms-jeopardy-winning-watson-computer-delving-into-medicine.

[92] Isabel Healthcare, "Press Release: United Hospital Adopts Isabel Healthcare for Its Diagnosis Decision Support," *PRWeb*, March 22, 2011, www.prweb.com/releases/2011/3/prweb8211181.htm.

[93] Jim Giles, "Watson Turns Medic: Supercomputer to Diagnose Disease," *New Scientist*, August 22, 2012, www.newscientist.com/article/mg21528796.400-watson-turns-medic-supercomputer-to-diagnose-disease.html.

[94] Steven Lohr, "I.B.M.'s Watson Goes to Medical School," *New York Times*, October 30, 2012, http://bits.blogs.nytimes.com/2012/10/30/i-b-m-s-watson-goes-to-medical-school.

[95] George J. Annas, "The Patient's Right to Safety—Improving the Quality of Care Through Litigation Against Hospitals," *New England Journal of Medicine*, May 11, 2006, 354(19):2063-6.

CHAPTER 9

SOCIAL NETWORKING

QUOTE

For decades, media companies have largely controlled the tools through which consumers were told what to buy, wear, or think. Now consumers possess the same ability to produce, distribute, and curate content—and distribute it to their peers in real time across social media platforms.

—Simon Mainwaring, branding consultant and social media specialist

VIGNETTE

Wanelo: Social Shopping Web Site Headed for Success

A **social shopping Web site** brings shoppers and sellers together in a social networking environment in which participants can share information and make recommendations while shopping online. On many social shopping Web sites, users can offer opinions on other members' purchases or potential purchases.

Wanelo (its name is a combination of *want*, *need*, and *love*) is a social shopping site that allows people to save a product found at any Web site to the user's account on the Wanelo site. Saving a product on Wanelo is similar to "liking" something on Facebook. Wanelo users save over 8 million items per day on the site. Each selection is saved in a product category such as coats, beauty products, home furnishings, or shoes. This enables Wanelo users to follow certain categories of products through the use of hashtags (which are essentially search keywords) such as *#shoes*.[1]

Wanelo has a trending products section that includes products popular across the site. In the site's "My Feed" section, Wanelo users can follow certain brands or stores, as well as other users, and they can comment on and discuss the products other people are saving. A user's "My Feed" section also highlights new products in the categories the user is following.[2] Users cannot purchase items they have saved at the Wanelo site. Instead, Wanelo users can click on any product on the site to be redirected back to the retail site where the item can be purchased. In some cases, Wanelo earns a commission from the operator of the e-commerce site on the purchase.[3]

The Web site receives about 1.3 million visitors each month, and most of those visitors are young women.[4] Approximately 90 percent of Wanelo members are women, and 60 percent of them are 24 or younger.[5] Many Wanelo users visit the site via a mobile app that enables them to save items, share their selections with others, and talk about products via their smartphone. Recently, the Wanelo app ranked number one in the lifestyle category at the Apple App Store, higher even than Amazon or eBay.[6]

In the five-month period from November 2012 to March 2013, the number of registered users grew from 1 million to 6 million.[7] With this kind of growth, Wanelo is having no problems attracting interest from venture capitalists. In early 2013, the company received $10 million in funding from a venture capitalist who valued the firm at over $100 million.[8]

Questions to Consider

1. Wanelo's CEO wants to continue to personalize the products that members see when they reach the site's homepage so as to encourage them to shop longer and share more items with their friends. Visit Wanelo's Web site (*http://wanelo.com*), and develop three ideas to help support this goal. What other improvement suggestions can you offer?
2. Would it be ethical for Wanelo to provide retailers with a list of the items saved by its members along with their email addresses so the retailers can market directly to Wanelo's members?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What are social networks, how do people use them, and what are some of their practical business uses?
2. What are some of the key ethical issues associated with the use of social networking Web sites?
3. What is a virtual life community, and what are some of the ethical issues associated with such a community?

WHAT IS A SOCIAL NETWORKING WEB SITE?

A **social networking Web site** creates an online community of Internet users that enables members to break down the barriers of time, distance, and cultural differences. Social networking Web sites allow people to interact with others online by sharing opinions, insights, information, interests, and experiences. Members of an online social network may use the site to interact with friends, family members, and colleagues—people they already know—but they may also make use of the site to develop new personal and professional relationships.

With over 2 billion Internet users worldwide, there is an endless range of interests represented online, and a correspondingly wide range of social networking Web sites catering to those interests. Thousands of social networking Web sites exist. Table 9-1 lists some of the most popular ones, based on the number of unique visitors per month.

TABLE 9-1 Popular social networking Web sites

Social networking Web site	Description	Estimated unique monthly visitors
Facebook	Social networking site for keeping up with friends, uploading photos, sharing links and videos, and meeting new people online	750 million
Tumblr	Microblogging platform and social network Web site that enables users to post multimedia and other content in short-form blog	300 million
Twitter	Real-time information service for friends, family members, and coworkers looking to stay connected through the exchange of messages that are a maximum of 140 characters	250 million
LinkedIn	Business-oriented social networking site used for professional networking; users create a network made up of people they know and trust in business	110 million

(Continued)

TABLE 9-1 Popular social networking Web sites *(Continued)*

Social networking Web site	Description	Estimated unique monthly visitors
Pinterest	Social networking site that allows members to pin photos, videos, and other items to their pin board to share with others	86 million
MySpace	General social networking Web site used by teenagers and adults worldwide; allows members to communicate with friends via personal profiles, blogs, and groups, as well as to post photos, music, and videos to their personal pages	70 million
Google+	Social network operated by Google that integrates social services such as Google Profiles and Google Buzz, and introduces new services such as Circles (enables users to organize contacts into groups for sharing), Hangouts (URLs used to facilitate group video chat), Sparks (enables users to identify topics in which they are interested), and Huddles (allows instant messaging within Circles)	65 million
Instagram	Online photo- and video-sharing social networking service	59 million
Live Journal	Social network where users can keep a blog, journal, or diary; also widely used to post political commentary	21 million
Tagged	Social network with a focus on helping members meet new people; suggests new friends based on shared interests; allows members to browse people, share tags and virtual gifts, and play games	25 million
Orkut	Social network for users to meet new and old friends and maintain existing friendships; it is very popular in Brazil and India, where it is one of the most frequently visited sites	18 million

Source Line: "Top 15 Most Popular Social Networking Websites/May 2013," eBiz/MBA, www.ebizmba.com/articles/social-networking-websites.

By some estimates, people spend about 20 percent of their time on PCs and 30 percent of their time on mobile devices accessing social networks. Averaged across all ages, U.S. males spend over 6 hours per month and females over 8 hours per month on social networking sites.[9] Of course, the social media phenomenon is not limited to the United States. Emarketer (an authority on digital marketing, media, and commerce) estimates the number of social network users worldwide to be 1.43 billion in 2012.[10] Figure 9-1 provides a look at the percentage of the population in select countries who visit social networks.

BUSINESS APPLICATIONS OF ONLINE SOCIAL NETWORKING

Although social networking Web sites are primarily used for nonbusiness purposes, a number of forward-thinking organizations are employing this technology to advertise, assess job candidates, and sell products and services. An increasing number of business-oriented social networking sites are designed to encourage and support relationships with

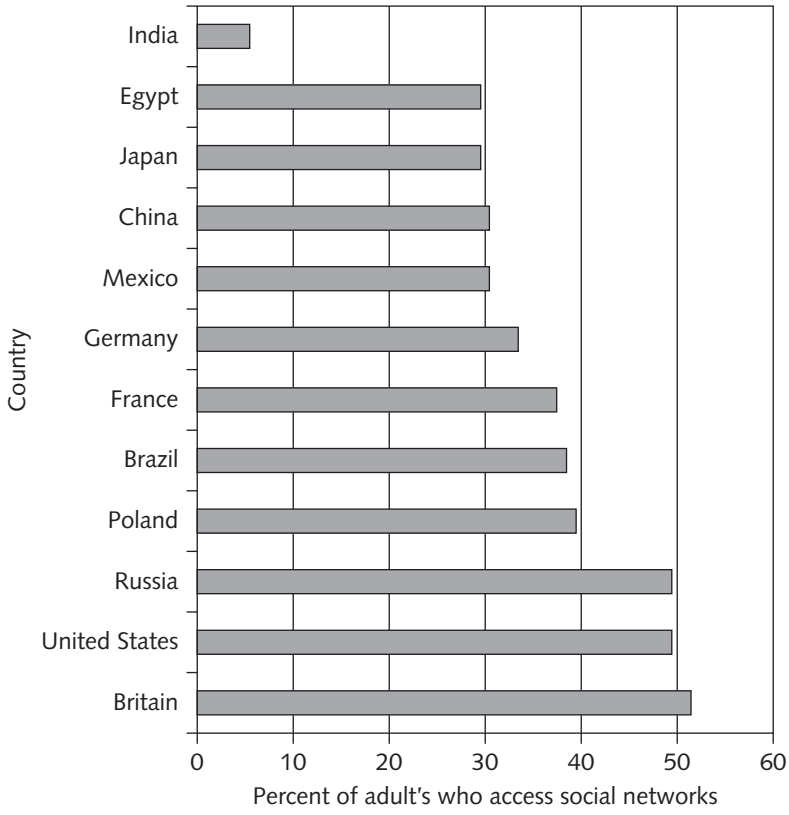


FIGURE 9-1 Global use of social networks

Source Line: Pew Research, "Global Attitudes Project," December 12, 2012, www.pewglobal.org/2012/12/12/social-networking-popular-across-globe.

consumers, clients, potential employees, suppliers, and business partners around the world, as shown in Table 9-2.

Social Network Advertising

Social network advertising involves the use of social networks to communicate and promote the benefits of products and services. Advertisers were quick to recognize the potential of social networking as another channel for promoting products and services. It is estimated that 89 percent of advertisers use free tools such as Facebook, Twitter, or Pinterest to promote their products. Additionally, 75 percent of advertisers use paid media such as ads on Facebook or sponsored blog content.[11] Social network advertising has become big business. Global social media advertising is expected to reach nearly $12 billion by 2014, with about half of that being spent in North America. The effectiveness of social network advertising varies by country. For example, Chinese users are three times more likely than Americans to make a purchasing decision based on what they see on a social network or in a blog, and a high percentage of Brazilians rely heavily on the use social media to identify new products and find special discounts.[12]

TABLE 9-2 Popular business-oriented social networks

Social networking Web site	Description
Biznik	Social networking site where entrepreneurs and small-business people collaborate to help each other to succeed
BT Tradespace	Site that brings businesses and customers together to buy, sell, share, and do business with people they can get to know and trust
FastPitch	Web site where professionals can make connections and markets their goods and services
Huddle	Networking site that can be used to manage projects, share files, and collaborate with people both inside and outside a company in a secure manner
LinkedIn	Site focused on helping professionals build and maintain a list of contacts; frequently used by job seekers and recruiters alike to link professionals with job opportunities
Ryze	Professional networking site targeted specifically at entrepreneurs, enabling them to build up a personal network and find new jobs; companies can also use Ryze to create a business community
Xing	Social network platform that helps professionals build and maintain a list of contacts; frequently used by job seekers and recruiters alike to link professionals with job opportunities

Source Line: Course Technology/Cengage Learning.

Two significant advantages of social network advertising over more traditional advertising media (e.g., radio, TV, and newspapers) are: (1) advertisers can create an opportunity to generate a conversation with viewers of the ad, and (2) ads can be targeted to reach people with the desired demographic characteristics.

The two primary objectives of social media advertisers are raising brand awareness and driving traffic to a Web site to increase product sales.[13] Organizations may employ one or more social network advertising strategies, several of which are detailed in the following sections.

Direct Advertising

Direct advertising involves placing banner ads on a social networking Web site. An ad can be displayed to every visitor to the Web site, or, by using the information in user profiles, an ad can be directed toward those members who would likely find the product most appealing. Thus, an ad for a new magazine on mountain biking could be directed to individuals on a social networking Web site who are male, who are 18 to 35 years old, and who express an interest in mountain biking. Others on the social networking Web site would not see the ad.

Advertising Using an Individual's Network of Friends

Companies can use social networking Web sites to advertise to an individual's network of contacts. When you sign on to your favorite social networking Web site, you might see a message saying, "Jared [your friend] just went to see *Hangover IV*—awesome, he says!" This can be an extremely persuasive message, as people frequently make decisions to do

something or purchase something based on input from their close group of friends. This might be a spontaneous message sent by Jared, or Jared might be getting paid by an online promotion firm to send messages about certain products. Or Jared might have simply "liked" the movie on Facebook, and his name is now being used in an endorsement for the movie. There are many ethical issues with this approach, as some people consider this to be exploiting an individual's personal relationships for the financial benefit of a company.

Indirect Advertising Through Groups

Innovative companies are also making use of a marketing technique by creating groups on social networking Web sites that interested users can join by becoming "fans." These groups can quickly grow in terms of numbers of fans to become a marketing tool for a company looking to market contests, promote new products, or simply increase brand awareness. Often, though, the fans gained in this manner do not remain loyal and are simply interested in earning discounts or special promotions.

The average adult consumer has "friended" or "liked" 29 brands on Facebook; however, only 39 percent of us interact with brands on a regular basis. The main reason for "friending" or "liking" is to access exclusive deals or offers.[14] A study by Syncapse, a social intelligence firm, found that each fan of a brand spent $116 more on the company than nonfans.

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, including the following:

- Coke has its own corporate blog called *Coca-Cola Conversations* that covers its brand history and provides information about Coca-Cola collectibles.
- Coke started a competition for the residents of the Second Life virtual world, challenging them to design a vending machine that dispenses the essence of Coke.
- The company placed a video on YouTube called "Mean Joe Greene—The Making of the Commercial," documenting the making of one of Coke's most famous TV commercials.
- Two fans of Coke, neither of whom had any official connection to the company, launched a Coca-Cola Facebook page in 2008. Within a few weeks, the page had attracted over 750,000 fans. As the number of fans grew into the millions, the page's creators agreed to turn over administration of the page to Coca-Cola.[15] The site is monitored by software filters for offensive words and phrases, and live moderators check its pages for anything truly offensive. Other than that, Coca-Cola managers generally let Facebook fans say what they want on the site.[16] The result has been nothing short of amazing. The Facebook fan page quickly grew to over 3 million fans worldwide."[17]
- In late 2010, Coca-Cola launched a nationwide campaign called Coke Secret Formula using SCVNGR (a social location-based gaming platform for mobile phones); the campaign encouraged young teens to look for hidden shopping experiences at shopping malls in the form of check-ins and photos. As participants completed challenges, they earned points toward American Express gift cards and Coke-branded merchandise.[18]

- Coca-Cola and Spotify, a music stream service, partnered in 2012 to integrate music into Coca-Cola's Facebook presence.[19]

All told, Coca-Cola has over 67 million Facebook likes, 3 million YouTube video content views, 204,000 LinkedIn followers, and 63,000 Twitter followers. 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.[20]

Company-Owned Social Networking Web Site

A variation on the above approach is for a company to form its own social networking Web site. For example, Dell created its own social networking Web site, IdeaStorm, in February 2007 as a means for its millions of customers in more than 100 countries to talk about what new products, services, or improvements they would like to see Dell develop. As of June 2013, the IdeaStorm community has suggested 19,075 ideas and posted 98,024 comments; Dell has implemented 537 customer-submitted ideas.[21]

Viral Marketing

Viral marketing 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. A successful viral marketing campaign requires little effort on the part of the advertiser; however, the success of such campaigns can be very difficult to predict. Hotmail created what is recognized by many as one of the most successful viral marketing campaigns ever when it first launched its service in 1996. Every email sent by a Hotmail user contained a short message at the end of the email that promoted Hotmail's free email service. As a result, almost 12 million new users signed up for Hotmail over a period of 18 months.[22] Another highly successful marketing campaign that went viral with 160 million views on YouTube was for Blendtec, a food blender, that is shown in a variety of videos blending everything from whole cooked chickens to iPads.[23]

The Use of Social Networks in the Hiring Process

A 2012 survey found that 92 percent of respondents either use or plan to use some form of social media—such as Facebook, LinkedIn, or Twitter—in their recruiting.[24] In addition, employers can and do look at the social networking profiles of job candidates when making hiring decisions. In an effort to thoroughly screen job applicants, some organizations ask for a candidate's username and password so they can log in as the candidate to Facebook or other social media networks. Of course, logging in as the candidate enables the interviewer to see everything posted to or about the candidate including details of their private user profiles. This practice is more common in the hiring of people for law enforcement positions, such as police officers or 911 dispatchers, so that the interviewer can check for possible gang affiliations or any photos or discussion of illegal or

questionable activity.[25] For a candidate desperate for a job, there is tremendous pressure to provide their logon information if requested.

There are varying opinions on the legality of this practice. Giving out Facebook login information violates the social network's terms of service. The Department of Justice regards it as a federal crime to enter a social networking site in violation of the terms of service. However, the agency has said such violations would not be prosecuted. A member of the American Civil Liberties Union has stated that employers are legally allowed to ask for access to social media accounts in the absence of laws specifically prohibiting the practice.[26]

Maryland was the first state to prohibit employers from asking current or prospective employees for their social network usernames or passwords. Six other states quickly followed suit in 2012, and over 30 states have proposed similar bills in 2013.[27]

Members of social networking Web sites frequently provide sex, age, marital status, sexual orientation, religion, and political affiliation data in their profile. 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 contents of the individual's social networking profile 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 Web 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 candidates should review their presence on social networking sites and remove photos and postings that reveal them in a potentially negative light. Many job seekers delete their Facebook or MySpace account 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.

The Use of Social Media to Improve Customer Service

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. Many consumer goods companies put toll-free 800 phone numbers on their products so that consumers could call in and speak with trained customer service reps to share their comments and complaints.

Increasingly, 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. A 2012 study found that 46 percent of Internet users had used social networks to express their frustration with poor products or services.[28] Customers also use social networks to seek advice on how to use products more effectively and how to deal with special situations encountered when

using a product. Unless organizations monitor social networks, their customers are 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 networks. 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. Here are a few examples of companies whose efforts have been effective in this area:

- Jet Blue has a customer service group that monitors Twitter on a 24×7 basis and responds immediately to tweets about operational problems. For example, social media monitors will call gate agents to suggest more information be announced if a customer tweets about a lack of information regarding a flight delay.[29]
- In 2009, GM formed a new customer service center, including five U.S. call centers that communicate with over 25,000 dealers and customers each day. The team also searches social media Web sites such as Facebook and Twitter looking for negative comments about the firm and its products and offering solutions to problems when possible.[30]
- Every day, Dell uses social media monitoring tools to track some 25,000 social media conversations that mention the brand, and the company participates in as many of these conversations as possible. Dell's goal is to listen to consumers, act on what it learns to introduce new products, improve its marketing, and provide better customer support. All this helps to retain customers and increase future sales.[31]
- The Capital Area Transportation Authority (CATA) operates 28 bus routes and provides over 11 million rides per year to the people of Lansing, Michigan.[32] CATA uses a social network monitoring program to monitor posts that its riders make on Facebook and Twitter. Employees reply to comments posted and also use riders' comments to manage its marketing message.[33]

Social Shopping Web Sites

Social shopping Web sites combine two highly popular online activities—shopping and social networking. Social shopping Web site members can typically build their own pages to collect information and photos about items in which they are interested. The social shopping Web site Stuffpit has 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.[34] Most social shopping Web sites generate revenue through retailer advertising. Some also earn money by sharing with retailers data about their members' likes and dislikes.

In addition to Stuffpit and Wanelo (which was discussed in the opening vignette), there are numerous other social shopping Web sites, a few of which are summarized in Table 9-3.

TABLE 9-3 Sample of social shopping Web sites

Web site	Description
Buzzillions	Product review Web site with over 17 million reviews across a wide range of products, with product rankings based on feedback from customers
Crowdstorm	Price comparison shopping resource that aggregates product information from various online buyers' guides, reviews, and blog postings
JustBoughtIT!	Facebook and Twitter app for capturing product recommendations from the online community; users can post a photo or screen shot online, share their purchases, and comment on what others are buying
Kaboodle	Social shopping site where members can discover, recommend, and share new products, provide advice, share feedback, get discounts, and locate bargains
MyDeco	Site with a focus on interior design and home decor; users can mock up virtual rooms using their favorite products
MyITThings	Both a fashion magazine and a shopping Web site that allows users to place products purchased in a virtual closet; users can store books, music, and other products
OSOYOU	UK-based social shopping site for women that aggregates products from 130 of the UK's top online stores selling fashion and beauty products
Zebo	A site that enables shoppers to chat, get tips, browse products, and conduct polls to get community input

Source Line: Course Technology/Cengage Learning.

Social shopping Web sites can be a great way for small businesses to boost their sales. Amenity Home—a tiny start-up with just three products, four employees, and no advertising budget—became a retailer on ThisNext.com, a social shopping Web site whose goal is to link shoppers with hard-to-find products. Shoppers at ThisNext.com found the Amenity Home products, copied photos of the products to their own blog pages, and brought the tiny firm some much-needed recognition. Amenity Home products started getting more and more hits on ThisNext.com, and the company has continued to grow and add more products to its online offerings.[35]

Retailers can purchase member data and comments from some social shopping Web sites 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.

SOCIAL NETWORKING ETHICAL ISSUES

When you have a community of tens of millions of users, 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 Web sites are cyberbullying, cyberstalking, encounters with sexual predators, and the uploading of inappropriate material.

Cyberbullying

Cyberbullying is the harassment, torment, humiliation, or threatening of one minor by another minor or group of minors via the Internet or cell phone. Based on a formal survey of 15,000 middle and high school children, it is estimated that as many as 25 percent of teenagers have experienced cyberbullying in their lifetime.[36]

Cyberbullying has sometimes become so intense that some children have committed suicide as a result:

- In 2010, a Rutgers freshman committed suicide after he learned his roommate used a webcam to film him having sex with another man and then posted the video to Twitter.[37]
- A 15-year-old California girl took her own life after photos of her being sexually assaulted were posted online and shared among her classmates in September 2012.[38]
- Friends of a 16-year-old Florida girl who hung herself in late 2012 say it was due to cyberbullying on the social networking Web site Ask.fm.[39]

Even with all these incidents of cyberbullying, as of April 2013, only 16 states have enacted cyberbullying laws while 5 others are considering such laws.[40] Most laws directed against cyberbullying focus on the school system as the most effective force and call on the school districts to develop policies regarding cyberbullying detection and punishment.[41]

There are numerous forms of cyberbullying, including the following:

- Sending mean-spirited or threatening messages to the victim
- Sending thousands of text messages to the victim's cell phone and running up a huge cell phone bill
- Impersonating the victim and sending inappropriate messages to others
- Stealing the victim's password and modifying his or her profile to include racist, homophobic, sexual, or other inappropriate data that offends others or attracts the attention of undesirable people
- Posting mean, personal, or false information about the victim in the cyberbully's blog or on a social networking page
- Creating a Web site or social networking profile whose purpose is to humiliate or threaten the victim
- Taking inappropriate photos of the victim and either posting them online or sending them to others via cell phone
- Setting up an Internet poll to elicit responses to embarrassing questions, such as "Who's the biggest geek in Miss Adams's homeroom?" and "Who is the biggest loser in the senior class?"
- Sending inappropriate messages while playing interactive games that enable participants to communicate with one another

Because cyberbullying can take many forms, it can be difficult to identify and stop. Ideally, minors would inform their parents if they became a victim of cyberbullying. Unfortunately, this does not happen often. When school authorities do get involved in an effort to discipline students for cyberbullying, they are sometimes sued for violating the student's right to free speech, especially if the activity occurred off school premises. As a result, some schools have modified their discipline policy to reserve the right to punish a student for actions taken off school premises if they adversely affect the safety and well-being of a student while in school.

All children should be educated about the potential serious impacts of cyberbullying, how to identify cyberbullying, and why it is important for them to refrain from cyberbullying. Children should be encouraged not to retaliate to mean-spirited messages, as doing so may cause the harassment to increase. Children need to understand that they can become inadvertent cyberbullies if they fail to think through the consequences of their actions. They should also be counseled against posting any data that is too personal, such as phone numbers, their home address, their school, or any other information that could allow a stranger to locate the child.

Cyberstalking

Cyberstalking is threatening behavior or unwanted advances directed at an adult using the Internet or other forms of online and electronic communications; it is the adult version of cyberbullying. Online stalking 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. In April 2013, a man was charged in federal court with cyberstalking 15 women in three different cities for several months. He told the women he had nude photos of them and that he would send them to their family and friends unless they sent him more naked photos of themselves.[42] And a former teacher was subjected to harassment and cyberstalking for over two years after he broke up with his girlfriend. The woman hacked into his email account and sent messages to his entire contact list posing as him and lying about how he had sex with underage students. She also posted nude photos of him on several Web sites.[43]

A recent survey concludes that 20 percent of Americans have been affected by cyberstalking.[44] In addition to federal laws, 45 states have passed laws prohibiting cyberstalking or have passed laws that include electronic forms of communication within traditional stalking or harassment laws.[45] Internet safety groups such as Working to Halt Online Abuse and Cyber Angels have documented increasing numbers of cyberstalking reports and requests for help from victims. In addition, many researchers feel that it is likely that the true extent of cyberstalking has been underestimated because the number of people online is increasing each year, and many cases still go unreported. See Table 9-4 for a list of federal laws designed to stop cyberstalking, as well an overview of gaps in those statutes.

TABLE 9-4 Federal laws addressing cyberstalking

Federal law	Scope	Gap
18 U.S.G. 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	The law does not address harassing phone calls to minors absent a showing of intent to entice or solicit the child for illicit sexual purposes.
18 U.S.G. 2261A	Makes it a federal crime for any person to travel across state lines with the intent to injure or harass another person	The requirement that the stalker physically travel across state lines makes the law largely inapplicable to cyberstalking cases.
47 U.S.C. 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	This law applies only to direct communications between the perpetrator and the victim; thus, it would not address a cyberstalking situation in which a person harasses or terrorizes another person by posting messages on a bulletin board or in a chat room encouraging others to harass or annoy another person.
18 U.S.C. 875(c)	Makes it a federal crime to transmit any communication in interstate or foreign commerce containing a threat to injure another person	This law applies only to communications of actual threats; thus, it would not apply in a situation where a cyberstalker engaged in a pattern of conduct intended to harass or annoy another (absent some threat); it is also not clear if it would apply to situations in which a person harasses or terrorizes another by posting messages on a bulletin board or in a chat room encouraging others to harass or annoy another person.

Source Line: "1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry," U.S. Department of Justice, www.justice.gov/criminal/cybercrime/cyberstalking.htm.

The National Center for Victims of Crime offers a detailed set of recommended actions for combating cyberstalking, including the following:

- When the offender is known, victims should send the stalker a written notice that their contact is unwanted and that all further contact must cease.
- Evidence of all contacts should be saved.
- Victims of cyberstalking should inform their Internet service provider (ISP) as well as the stalker's ISP, if possible.
- Victims should consider speaking to law enforcement officers.
- Above all else, victims of cyberstalking should never agree to meet with the stalker to "talk things out."[46]

Encounters with Sexual Predators

Some social networking Web sites have been criticized for not doing enough to protect minors from encounters with sexual predators. MySpace spent two years purging potential problem members from its site, including 90,000 registered sex offenders banned from the

site in early 2009.[47] (As of January 2012, there were approximately 747,400 registered sex offenders in the United States.[48]) According to Connecticut's then-Attorney General Richard Blumenthal, "convicted sex offenders mixing with children on MySpace ... is absolutely appalling and totally unacceptable." During his time in office, Blumenthal worked with other officials to push social networking Web sites to adopt stronger safety measures.[49]

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. Several states have laws that specify that certain information must be collected when a sex offender registers for use of a social network.[50]

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 requires the formation of state sex offender Web sites. 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 Web sites 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.[51] The act was named after an 11-year-old Minnesota boy who was abducted in 1989 and remains missing.

The 2006 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 for which sex offenders must register and what data must be captured, as shown in Table 9-5.[52]

TABLE 9-5 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

Source Line: Course Technology/Cengage Learning.

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 9-6.[53] The act was named for Adam Walsh, a young boy abducted from a Florida shopping mall and later found murdered.

TABLE 9-6 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

Source Line: Course Technology/Cengage Learning.

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, 5 U.S. territories, 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 January 2013, only 17 jurisdictions had implemented the SORNA requirements of the Adam Walsh Act. Law enforcement agencies point out that their workload has increased due to the increased frequency at which 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.[54]

Uploading of Inappropriate Material

Most social networking Web sites have policies against uploading videos depicting violence or obscenity. Facebook, MySpace, and most other social networking Web sites have terms of use agreements, a privacy policy, or a content code of conduct that summarizes key legal aspects regarding use of the Web site. Typically, the terms state that the Web site has the right to delete material and terminate user accounts that violate the site's policies. The policies set specific limits on content that is sexually explicit, defamatory, hateful, or violent, or that promotes illegal activity.

Policies do not stop all members of the community from attempting to post inappropriate material, and most Web sites do not have sufficient resources to review all material submitted for posting. For example, more than 100 hours of video are uploaded to YouTube every minute (this is the equivalent of approximately 670,000 full-length movies each week). Quite often, it is only after other members of a social networking Web site complain about objectionable material that such material is taken down. This can be days or even weeks. Ideally, reviewers would also look at the text content submitted to a networking site—not just photos and videos. A posting to a teenage-oriented Web site may advocate underage drinking, sex, and drug use but may not use photos or videos to do so.

Individuals who appear in photos or videos doing inappropriate or illegal things may find themselves in trouble with authorities if those photos and videos end up on the Internet:

- U.S. Representative Anthony Weiner was forced to resign in 2011 after admitting he sent sexually explicit photos of himself to several women using social networks, including Facebook and Twitter.[55]

- Seven Pennsylvania students filmed themselves beating and attempting to hang another 13-year-old student. (The term *wolfpacking* is used to describe such acts of violence by gangs of bullies.) The students were arrested for alleged kidnapping and assault.[56]
- A brutal beating of a one-year-old pit bull was captured on a cell phone camera and posted on YouTube. Police were able to use the video to quickly track down the person responsible for the beating. The individual was arrested and charged with animal cruelty. The dog was taken into custody by the Society for the Prevention of Cruelty to Animals (SPGA).[57]
- A third-year political science student at the University of California, Los Angeles withdrew from the school after she posted her video rant against Asian students on YouTube. The student was complaining about Asian students in the school library using their cell phones to reach family members after the tsunami in Japan.[58]

ONLINE VIRTUAL WORLDS

An **online virtual world** is a shared multimedia, computer-generated environment in which users, represented by avatars, can act, communicate, create, retain ownership of what they create, and exchange assets, including currency, with each other. An **avatar** (see Figure 9-2) is a character in the form or a human, animal, or mythical creature.

FIGURE 9-2 An avatar is a representation of a virtual world visitor
Credit: © Ralf Juergen Kraft/Shutterstock.com

Virtual worlds are usually thought of as alternative worlds where visitors go to entertain themselves and interact with others. CityVille, Entropia Universe, FarmVille, and Second Life are all examples of online virtual worlds.

One type of online virtual world, a **massively multiplayer online game (MMOG)**, is a multiplayer video game capable of supporting hundreds and even thousands of concurrent players. The games are accessible via the Internet, with players using personal computers; game consoles such as Xbox 360, Wii, and PlayStation 3; and even smartphones. **Massive multiplayer online role-playing games (MMORPG)** is a subcategory of MMOG that provides a huge online world in which players take on the role of a character and control that character's action. Characters can interact with one another to compete in online games and challenges that unfold according to the online world's rules and storyline. Happy Farm, Minecraft, and World of Warcraft are popular MMOGs.

Avatars in many virtual worlds can shop, hold jobs, run for political office, develop relationships with other avatars, take a test drive in a virtual world car, and even engage in criminal activities. Avatars may promote events and hold them in the virtual world (e.g., garage sales, concerts, conferences). Avatars can even start up new businesses and create or purchase new entities, such as houses, furnishings for their houses, clothing, jewelry, and other products. Avatars use the virtual world's currency to purchase goods and services in the virtual world. The value of objects in a virtual world is usually related to their usefulness and the difficulty of obtaining them. The ownership of such items is recognized by other avatars in the virtual world—for example, this is John's house; others may not occupy it without his permission.

Avatars can earn virtual world money by performing tasks in the virtual world, or their owners can purchase virtual world money for them using real world cash. In some virtual worlds, avatars can convert their virtual world money back into real dollars at whatever the going exchange rate is by using their credit card at online currency exchanges. Virtual world items may also be sold to other virtual world players for real world money. For example, John Jacobs, whose avatar is the character Neverdie in the Entropia Universe MMOG, sold his Club Neverdie on the virtual asteroid orbiting Planet Calypso for $635,000.[59] It is estimated that the U.S. virtual goods market was $1.6 billion in 2010, and the total worldwide market may have been as much as $10 billion.[60]

Crime in Virtual Worlds

It seems the freedom and anonymity afforded avatars in a virtual world encourages some individuals to unleash their darker side. Thus, virtual worlds raise many interesting questions regarding what is a criminal act and whether law enforcement—real or virtual—should get involved in acts that occur in virtual worlds.

Some virtual activities are clear violations of real world law and need to be reported to law enforcement authorities—for example, avatars trafficking in actual drugs or stolen credit cards. Other virtual activities, such as online muggings and sex crimes, can cause real life anguish for the human owners of the avatars involved but generally do not rise to the level of a real life crime. Although most virtual worlds have rules against offensive behavior in public, such as using racial slurs or performing overtly sexual actions, consenting adults can travel to private areas and engage in all sorts of socially unacceptable behavior. Bad deeds done online are often mediated by the game administrators, who can

take action according to the rules of the game and with consequences internal to the game.

Some virtual world activities fall into a vast gray area. For example, in the real world, gambling games within casinos are inspected and regulated by state gaming commissions to ensure that the games are "fair." However, such regulations do not exist in the virtual world, and the potential for unfair games stacked in favor of the operator is high.

Educational and Business Uses of Virtual Worlds

Virtual online worlds are also being used for education and business purposes. The New Media Consortium (NMC) is an international consortium of hundreds of colleges, universities, museums, and research centers exploring the use of new media and technologies to improve teaching, learning, and creative expression. Members of NMC can conduct classes and meetings from within a growing number of virtual learning worlds. They can also build custom virtual learning worlds, simulations, and learning games. The virtual reality experience provides participants with a real sense of being there when attending a virtual class or conference. Experienced designers can develop virtual classes that immerse and engage students in the same way that today's video games grab and keep the attention of players.

Second Life Work Microsites enable businesses and government agencies to use Second Life for virtual meetings, events, training, and simulations to stimulate innovation while minimizing the cost and environmental impact of travel. Second Life Education Microsites are designed for educators who want to offer virtual education options to augment their traditional curriculum.

Germany's TUV NORD Group is an international provider of technology security solutions—including certification and testing—with 8,500 employees in over 70 countries. The firm began using Second Life in 2007 to recruit, conduct meetings, and hold game-based education.

Chevron—a U.S. multinational company engaged in the gas, oil, and geothermal industries—is using a virtual world model of its Salt Lake refinery for training new operators, some of whom have never even been in a refinery unit. Trainees guide their avatars through a 3D virtual model of the refinery to learn the basics of safe operation and how to deal with typical operational issues. Practicing in the virtual environment enables trainees to be exposed to many more operations scenarios in much less time than waiting for similar situations to arise in the real world.[61]

Summary

- A social networking Web site 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.
- By some estimates, people spend about 20 percent of their time on PCs and 30 percent of their time on mobile devices accessing social networks.
- An increasing number of business-oriented social networking sites are designed to encourage and support relationships with consumers, clients, potential employees, suppliers, and business partners around the world.
- Social network advertising enables advertisers to generate a conversation with viewers of their ads and to target ads to reach people with the desired demographic characteristics. The two primary objectives of social media advertisers are raising brand awareness and driving traffic to a Web site to increase product sales.
- There are several social network advertising strategies, including direct advertising, advertising using an individual's network of friends, indirect advertising through social networking groups, advertising via company-owned social networking Web sites, and viral marketing.
- Employers often look at the social networking Web site profiles of job candidates when making hiring decisions.
- 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 candidates who use social networking Web sites should review and make appropriate changes to their profiles before starting a job search.
- Many organizations monitor social media networks as a means of improving customer service, retaining customers, and increasing sales.
- A social shopping Web site brings shoppers and sellers together in a social networking environment in which members share information and make recommendations while shopping online.
- Cyberbullying is the harassment, torment, humiliation, or threatening of one minor by another minor or group of minors via the Internet or cell phone. It is estimated that as many as 25 percent of teenagers have experienced cyberbullying in their lifetime.
- Cyberstalking is threatening behavior or unwanted advances directed at an adult using the Internet or other forms of online and electronic communications; it is the adult version of cyberbullying.
- Although current federal statutes address some forms of cyberstalking, there are still large gaps in current federal and state law.
- There are over 747,000 registered sex offenders in the United States; 90,000 of them were onetime members of MySpace.
- Many social networking Web sites have policies against uploading violent or obscene material; however, these policies are difficult to enforce.

- An online virtual world is a shared multimedia, computer-generated environment in which users, represented by avatars, can act, communicate, create, retain ownership of what they create, and exchange assets, including currency.
- Virtual worlds raise many interesting questions regarding what is a criminal act and whether law enforcement, real or virtual, should get involved in acts that occur in virtual worlds.
- Virtual online worlds are increasingly being used for education and business purposes.

Key Terms

avatar
cyberbullying
cyberstalking
massively multiplayer online game (MMOG)
massive multiplayer online role-playing games (MMORPG)
online virtual world
social network advertising
social networking Web site
social shopping Web site
viral marketing

Self-Assessment Questions

The answers to the Self-Assessment Questions can be found in Appendix B.

1. A(n) _____ brings shoppers and sellers together in a social networking environment in which participants can share information and make recommendations while shopping online.
2. How many people are estimated to be Internet users worldwide?
   a. over 1 billion
   b. about 1.5 billion
   c. over 2 billion
   d. over 3 billion
3. _____ is a popular business-oriented Web site used for professional networking, with over 100 million unique visitors each month.
4. Averaged across all ages, U.S. males spend over 6 hours per month and females over 8 hours per month on social networking sites. True or False?
5. _____ 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.
   a. direct advertising
   b. viral marketing
   c. indirect advertising through groups
   d. a company-owned social networking Web site

6. Employers can legally reject a job applicant based on the content of the individual's social networking Web site as long as the company is not violating discrimination laws. True or False?
7. There are over 747,000 registered sex offenders in the United States, and 90,000 of them were found on and subsequently banned from the social networking Web site _____.
8. Based on a formal survey of 15,000 middle and high school children, it is estimated that as many as 45 percent of teenagers have experienced cyberbullying in their lifetime. True or False?
9. Current federal statutes thoroughly address all aspects of cyberstalking, with no gaps in federal and state laws. True or False?
10. Which of the following measures is employed by social networking Web sites to avoid the posting of objectionable material?
    a. The terms of use agreement for most social networking Web sites states that the Web site reserves the right to delete material or terminate user accounts that violate the site's policies.
    b. Social networking Web sites employ people to review material submitted.
    c. Other users sometimes report objectionable material.
    d. All of the above
11. To date, no practical business applications of online virtual worlds have been implemented. True or False?
12. The two primary objectives of social media advertisers are driving traffic to a Web site to increase product sales and raising _____.

Discussion Questions

1. 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 instant 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 Facebook, Twitter, and instant messaging have led to more communications, not less. What do you think?
2. Keep track of the time that you spend on social networking Web sites for one week. Do you think that this is time well spent? Why or why not?
3. Do you think that college instructor-student friendships on social networking Web sites are appropriate? Why or why not?
4. Develop an idea for a social media marketing campaign for one of your favorite consumer products. Document how you would turn your message viral.
5. Discuss the following idea: The information posted on social networking Web sites about news events occurring in foreign countries is an excellent source of up-to-the-minute news.
6. Identify two significant advantages that social network advertising has over other forms of advertising.

7. What advice would you give a friend who is the victim of cyberstalking?
8. In 2011, over 3,330 people were killed and 387,000 people were injured in auto crashes involving a distracted driver. Additionally, 40% of U.S. teenagers report being in a car when the driver used a cell phone in such a manner that it put the passengers at risk.[62] Do you think that more needs to be done to discourage the use of cell phones and smartphones when driving? If so, what additional actions could be taken? If not, why not?
9. What measures would you use to gauge the success of a social networking promotion designed to get people to try a new consumer product?
10. Can role playing illegal and violent fantasies in a virtual world affect individuals and society in the real world? What are the social and ethical implications of such role playing? Should limits be placed on what players can do in virtual worlds?
11. Do a search of the Web and develop a list of six companies that have created their own social networking Web sites.
12. 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.
13. Review your user profile on your most frequently used social networking Web site. Do you think you need to make any changes to this profile? If so, what changes?
14. Check out the privacy policy of three social shopping Web sites 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 30 minutes into a job interview for your dream job—one where your college education and experience could really be applied. So far everything is going well. Then, the interviewer asks you to write down your Facebook user name and password so she can do further research after the formal interview is over. What would you do?
2. A coworker who is a recruiter told you that she is going to drop a job candidate because she feels that he is totally irresponsible. She found out through research on Facebook that the candidate married and divorced his high school sweetheart before graduating from college and once had his car repossessed. What would you say to your coworker about this?
3. Your friend has been active on the Wanelo social shopping site. He joined with a fictitious name and personal information, and is posing as a young twentysomething female. He is "following" half a dozen young women and making derisive comments on the collections of items they have saved. He has shown you a number of his postings and the associated—sometimes angry, sometimes hurt—responses. He invites you to join him in his charade. What would you do?
4. You are surprised to receive Facebook and LinkedIn friend requests from one of your neighbors in the apartment building that you moved into last weekend. You know nothing about the

individual and are really not interested in being friends. Your first reaction is to ignore the requests, but you are concerned that you will keep running into the person around your apartment complex and that the situation could become awkward. What would you do?

5. You are a new hire at a firm that manufactures and markets athletic equipment. You and several other new employees have been asked by your employer to begin posting positive messages about your company's latest product—a $225 running shoe with state-of-the-art features—on Facebook, Stuffpit, and Twitter. While you are interested in the product, you cannot afford to buy it and have never tried it. Your manager says not to worry, the Marketing Department will provide you with prewritten statements for you to post. What would you do?
6. You have just received a second invitation to join John's friend list. You met John three weeks ago at a group study session prior to last semester's Calculus II finals. He came across as very quiet and sort of strange. You did nothing to encourage his attention, but now you keep running into him at the oddest places and strangest times—at the self-service car wash, the 24-hour gym at 1:00 a.m., and the bakery at 7:00 a.m. He always flashes you a smile but has nothing to say. You think you've caught him taking snapshots of you a couple of times with his cell phone. He is starting to creep you out. What would you do?
7. A friend of yours has asked you to help him and a group of three or four others shoot a video and upload it to YouTube. The subject of the video is "Happenings at Work," and it will include several vignettes about funny incidents at work. What would you do?
8. You are a new player in Second Life and are surprised when another avatar asks if you want to buy some marijuana. You are not sure if the person is merely role playing or is serious. What would you do?

Cases

1. Procter & Gamble Turns to Social Networking

Spending big on advertising has always been a key strategy for consumer products giant Procter & Gamble (P&G). With recent annual global ad spending over $9 billion, P&G is one of the world's top advertisers.[63] P&G was an early sponsor and producer of daytime radio and TV dramas—for which the term *soap opera* was coined. Its *Guiding Light* program began airing on radio in 1937 and moved to TV in 1952.[64] The P&G produced and sponsored *As the World Turns*, which was the leading soap opera for decades, winning many daytime Emmy awards. However, over the years, women—the target audience for such programs—made a huge shift in their TV viewing habits as they moved into the workplace, became more interested in talk and reality shows, and, more recently, began spending more of their leisure time online. P&G finally pulled the plug on *As the World Turns* in 2010 after 53 years.[65]

In 2006, P&G began working with Facebook to promote its brands using standard banner ads and promoting Facebook groups seeking fans for the company or its products. However, this approach was not very successful. P&G's biggest success was a Crest Whitestrips promotion that invited college students to become "fans" on its Facebook page. The company offered thousands of free movie screenings and sponsored concerts but still only attracted 14,000 fans to the product's Facebook page. When the promotions ended, the fans left too. The problem,

according to Web guru Seth Goldstein, is: "Advertisers distract users; users ignore advertisers; advertisers distract better; users ignore better."[66]

P&G's next experiment with social networking was in 2007, when it collaborated with Yahoo! and the ZiZi Group to create Capessa.com, an online social network targeted at women. Capessa enabled women to post their stories and discuss topics such as parenting, managing their careers, getting in shape, and dealing with illnesses. One of the goals of this experiment was to identify ways in which social networking could be used to gain a better understanding of women's likes, dislikes, interests, and needs. Ultimately, no direct connection between Capessa and an increase in sales could be made.[67] That may be, in part, because some users are skeptical as to whether the stories posted on social networks are from real people or from paid actors or authors.[68]

Recognizing that its current approach was not working, P&G invited Google, Facebook, Twitter, and other social media experts to work with it to explore how online and digital media could more effectively support its marketing program. This spawned several new approaches. P&G has expanded its efforts to sell some top brands (Pampers, Olay, and Pantene) by offering shopping through a Facebook app. Consumers click a Shop Now tab on the page to complete their orders and then check out through Amazon.com.[69] And its "Smell Like a Man, Man" commercials began appearing on YouTube. These commercials starred the beefy ex-football player Isaiah Mustafa wearing only a towel. The commercials were a big hit, drawing over 140 million views and helping its Old Spice brand sales to expand at a double-digit growth rate.[70]

As a result of these successes, P&G set a goal that each of its brands develop a meaningful presence on Facebook. In addition, it is creating smartphone applications for its consumers; one free app available at Apple's App Store and Google's Android Market provides women with guidance on which P&G beauty products to use and how to use them to get a desired look.[71] Marketing experts say many of the large companies were slow to adopt the use of social networks; however, they also agree that consumer goods companies Coca-Cola, Pepsi, P&G, Unilever, and Johnson & Johnson are now coming on strong.[72] The decision to drop soap operas and move advertising dollars to social media was not a popular one with some senior P&G managers (who had spent much of their careers supporting advertising on soap operas) nor with many soap opera fans (who were very attached to these programs), but the decision was a clear indication that P&G recognizes that "the times they are a-changing."

Discussion Questions

1. Should the success of a social networking marketing campaign be measured simply by an increase in units sold? Why or why not?
2. What key arguments might have been used to convince P&G marketing executives to drop their long-running use of soap operas and replace them with social network advertising?
3. Develop a list of five key criteria that P&G might use to assess both the appropriateness and effectiveness of its YouTube commercials.

2. Social Networks for Chronic Health Condition Sufferers

For people living with chronic health conditions (one that is persistent and long lasting, such as arthritis, asthma, high blood pressure, cancer, or HIV/AIDS), social networking can play an

important role. A 2010 national telephone survey of 3,001 adults found that 23 percent of Internet users living with a chronic health condition have gone online to find others with similar health conditions and to share experiences and seek information.[73] Indeed, there are a number of patient networking sites that enable users to connect directly to one another based on medical condition, including Alliance Health Networks, CureTogether, DiabeticConnect, Disaboom, FacetoFace Health, HealthCentral, Inspire, and PatientsLikeMe. Some chronic conditions sufferers have even taken the initiative to start their own social networking sites focused on their condition by using social network creation services, such as Ning.

Some patients use social networking to discover no-nonsense tips about coping with their disease or disability that physicians and their family cannot provide simply because they have not lived with it (for example, which restaurants and movie theaters have the best wheelchair access). Others network to become better informed about their condition and long-term prognosis, learn about alternative or experimental drugs and treatments, or discuss medical costs and insurance. Certainly doctors, nurses, and other health professionals should continue to be the primary source of health information, but social networks can be a useful source of information as well.

Many patients network as a means to deal with the anxiety, depression, and stress that frequently accompany chronic conditions. For example, Sean Fogerty, a 50-year-old with multiple sclerosis who is recovering from brain cancer, spends over an hour most nights chatting online with other patients. Sean says social networking has "literally saved my life, just to be able to connect with other people."[74]

Social networking sites targeted at those suffering from chronic health conditions do raise some potential ethical concerns. Obviously people must be cautious about sharing too much private health information and personal data online, especially among a group of often anonymous users. There is also a risk that members of the group may unwittingly share erroneous or out-of-date information on which others may act. In addition, if the general tone of the network site is overly pessimistic about the chronic condition, participants can experience an even deeper depression over their situation. Thus although such social networking sites have the potential to help sufferers with chronic health conditions, they must be used with care.

Discussion Questions

1. Imagine that your grandmother has suffered from asthma all her life and within the past year was diagnosed with type II diabetes. She has been quite depressed as she must now be extremely careful with her diet, administer insulin shots to herself before each meal, and take two types of oral medication. She hates sticking herself to take her sugar level two or three times a day and has found it difficult to watch her diet and keep her blood sugar level within normal ranges. Would you suggest she join a social network for people with diabetes? Why or why not?
2. Do research and try to find social networks that are designed for people who suffer from alcohol, drug, or gambling addiction. Are there additional potential ethical issues for social networking sites targeted at those suffering from an addiction? Write a brief paragraph or two summarizing your findings.
3. What issues might arise trying to discuss with your primary care physician an experimental treatment or drug you discovered on a social network? How might you be able to broach this topic without upsetting your physician?

3. Facebook Raises Privacy Issues

Since its founding in 2004, Facebook has changed dramatically—expanding from a tiny start-up firm to an Internet powerhouse, with a market value over $60 billion and revenue in excess of $5 billion in 2012.[75,76]

Facebook has also changed the way it manages its users' privacy—going from being a private Web site where you could communicate with just the people you chose to becoming a forum where much of your information is made public. An excerpt from the earliest Facebook privacy policy reads: *No personal information that you submit to Facebook will be available to any user of the Web site who does not belong to at least one of the groups specified by you in your privacy settings.*[77] Contrast this with an excerpt from Facebook's privacy policy in 2013: *When you connect with a game, application or website…we give the game, application, or website… your basic info (we sometimes call this your "public profile"), which includes your User ID and your public information. We also give them your friends' User IDs (also called your friend list) as part of your basic info.* This change in its approach to privacy is causing Facebook to undergo increasing scrutiny of its policies and actions in terms of safeguarding the information of its more than 750 million active monthly users.[78]

Most of the Facebook applications, or *apps,* that enable users to play games and share common interests are created by independent software developers. In 2010, it was uncovered that many of these apps (e.g., FarmVille, Texas HoldEm, and FrontierVille) were transmitting users' unique Facebook user IDs to at least two dozen marketing and database firms, where they were used to build profiles on users' online activities.[79]

Because a Facebook user ID is a public part of all Facebook profiles, knowledge of user IDs enables a company to determine the users' names even if they set all their Facebook information to be private; companies can simply perform a search using the ID to find the person's name. The user IDs may also reveal the users' age, address, and occupation, and can allow a company to access photos for those users who did not specify the most restrictive privacy setting. At least one of the companies linked the Facebook data to its own database of Internet users' data, which it sells to other marketers.

Interestingly, Facebook prohibits app developers from sharing data about users to outside marketing and database companies. However, it has been difficult for Facebook to enforce its rules for the more than half million apps that run on its Web site. Facebook itself was caught transmitting user ID numbers under certain conditions when users clicked on an ad; Facebook discontinued the practice after it was reported in the press.[80]

In December 2010, Facebook implemented a new Tag Suggestions feature for photos. When users add photos to their Facebook pages, the Tag Suggestions feature uses facial recognition software to suggest the names of people in the photos based on photos in which they have already been tagged. It is estimated that more than 100 million people tag photos every day on Facebook.[81] Although users could always tag photos of their Facebook "Friends," the Tag Suggestions feature process is now semiautomated, with Facebook providing suggestions regarding which of your friends is in a photo.[82]

Initially the feature was made available to just users in the United States, perhaps because the privacy laws in many other countries are much stricter. However, within five months, Facebook began to roll out the Tag Suggestions feature worldwide. European Union data protection regulators are now studying the new feature for possible privacy rule violations.[83]

Facebook also changed its users' privacy settings to make the facial recognition feature a default; users must opt out of having their names suggested for photos by changing their privacy settings to disable the feature. However, Facebook does not give its users the option not to be tagged in any photos; a user's Facebook Friends can still tag a user in a photo manually, even if the user has disabled the Tag Suggestions feature. Users who do not want their name associated with a photo must manually "untag" themselves in each photo. This approach of automatically enrolling users into new features without their knowledge or consent has become standard practice for the firm as a means of ensuring that users experience the full effects of Facebook.[84] Facebook temporarily suspended Tag Suggestions in 2012, but in early 2013, the site reenabled it in the United States after making what the company called "technical improvements" to the feature.[85]

Google had developed similar facial recognition technology for smartphones for its Google Goggles application, but did not release the facial recognition portion of that app. Google chairman Eric Schmidt said: "As far as I know, it's the only technology that Google built and after looking at it, we decided to stop. People could use this stuff in a very, very bad way as well as in a good way."[86]

Discussion Questions

1. Do you agree with Facebook's philosophy of automatically enrolling users in new features without their knowledge or consent? Why or why not?
2. What concerns might a Facebook user have with the Tag Suggestions feature?
3. Do you use the Facebook Photo Tag Suggestions feature? Why or why not?

End Notes

[1] Tomio Geron, "Inside Wanelo, the Hot Social Shopping Service," *Forbes*, March 27, 2013, www.forbes.com/sites/tomiogeron/2013/03/27/inside-wanelo-the-hot-social-shopping-service.

[2] Tomio Geron, "Inside Wanelo, the Hot Social Shopping Service," *Forbes*, March 27, 2013, www.forbes.com/sites/tomiogeron/2013/03/27/inside-wanelo-the-hot-social-shopping-service.

[3] Tomio Geron, "Inside Wanelo, the Hot Social Shopping Service," *Forbes*, March 27, 2013, www.forbes.com/sites/tomiogeron/2013/03/27/inside-wanelo-the-hot-social-shopping-service.

[4] Jenna Worthham, "Wanelo: Social Commerce Site Is Big with Young Shoppers," *New York Times*, January 24, 2013, http://bits.blogs.nytimes.com/2013/01/24/a-look-at-wanelo-a-social-commerce-site-for-younger-shoppers.

[5] Liz Gannes, "Meet Deena Varshavskaya, CEO of Social Shopping Sensation Wanelo," *All Things D*, April 30, 2013, http://allthingsd.com/20130430/meet-deena-varshavskaya-ceo-of-social-shopping-sensation-wanelo.

[6] Jenna Worthham, "Wanelo: Social Commerce Site Is Big with Young Shoppers," *New York Times*, January 24, 2013, http://bits.blogs.nytimes.com/2013/01/24/a-look-at-wanelo-a-social-commerce-site-for-younger-shoppers.

[7] Tomio Geron, "Inside Wanelo, the Hot Social Shopping Service," *Forbes*, March 27, 2013, www.forbes.com/sites/tomiogeron/2013/03/27/inside-wanelo-the-hot-social-shopping-service.

[8] Tomio Geron, "Inside Wanelo, the Hot Social Shopping Service," *Forbes*, March 27, 2013, www.forbes.com/sites/tomiogeron/2013/03/27/inside-wanelo-the-hot-social-shopping-service.

[9] Nielsen, "State of the Media: The Social Media Report 2012," December 4, 2012, www.nielsen.com/us/en/reports/2012/state-of-the-media-the-social-media-report-2012.html.

[10] Christian Arno, "Worldwide Social Media Usage Trends 2012," *Search Engine Watch*, December 26, 2012, http://searchenginewatch.com/article/2167518/Worldwide-Social-Media-Usage-Trends-in-2012.

[11] Nielsen, "The Paid Social Media Advertising Report 2013," January 25, 2013, www.nielsen.com/us/en/reports/2013/the-paid-social-media-advertising-report-2013.html.

[12] Katie Lepi, "How Social Media Is Used Around the World," *edudemic*, February 28, 2013, http://edudemic.com/2013/02/how-social-media-is-used-around-the-world.

[13] "Social Media Advertising—Spending Statistics and Trends," GoGulf.com, April 5, 2013, www.go-gulf.com/blog/social-media-advertising.

[14] Lucia Moses, "Data Points: Brand Fans," *AdWeek*, January 16, 2013, www.adweek.com/news/advertising-branding/data-points-brand-fans-146447.

[15] Joe Guy Collier, "Coke Fans' Facebook Page Draws Millions of Users," *Atlanta Journal-Constitution*, March 30, 2009, www.ajc.com/business/content/business/coke/stories/2009/03/30/coke_facebook_page.html.

[16] Theresa Howard, "Seeking Teens, Marketers Take Risks by Emulating MySpace," *USA Today*, May 22, 2006, www.usatoday.com/tech/news/2006-05-01-myspace-marketers_x.htm.

[17] "How Fortune 1000 Companies Are Harnessing the Power of Social Media," White Paper, 2009, www.scribd.com/doc/18557214/How-Fortune-1000-Companies-Are-Harnessing-the-Power-of-Social-Media.

[18] Jennifer Van Grove, "Coke Targets Teens with Black Friday SCVNGR Promotion," *Mashable*, November 18, 2010, http://mashable.com/2010/11/19/scvngr-coke-rewards.

[19] Andy Fixmer and Edmund Lee, "Coca-Cola Teams Up with Spotify in Music-Sharing Deal," *Bloomberg Businessweek*, April 18, 2012, www.businessweek.com/printer/articles/48160?type=bloomberg.

[20] "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.

[21] "Dell Idea Storm," www.ideastorm.com/idea2ExploreMore?v=1367209206230&Type=AllIdeas&Filter=IdeaStorm (accessed June 19, 2013).

[22] Dr. Ralph F. Wilson, "The Six Simple Principles of Viral Marketing," *Web Marketing Today*, February 1, 2005, www.wilsonweb.com/wmt5/viral-principles.htm.

[23] "7 Great Viral Marketing Campaigns," *Inc*., www.inc.com/ss/7-successful-viral-marketing-campaigns#4 (accessed May 5, 2013).

[24] Darrell Smith, "Job Front: Social Media Expected to Play Bigger Role in Hiring," *Sacramento Bee*, February 4, 2013, www.sacbee.com/2013/02/04/5162867/job-front-social-media-expected.html.

[25] Manuel Valdes and Shannon McFarland, "Job Seekers' Facebook Passwords Asked for During U.S. Interviews," *Huffington Post*, March 20, 2012, www.huffingtonpost.com/2012/03/20/facebook-passwords-job-seekers_n_1366577.html.

[26] Katy Steinmetz, "States Rush to Ban Employers from Asking for Social Media Passwords," *Time*, April 9, 2013, http://swampland.time. com/2013/04/09/states-rush-to-ban-employers-from-asking-for-social-media-passwords.

[27] Katy Steinmetz, "States Rush to Ban Employers from Asking for Social Media Passwords," *Time*, April 9, 2013, http://swampland.time.com/2013/04/09/states-rush-to-ban-employers-from-asking-for-social-media-passwords.

[28] Brian Solis, "The First Mile: The Broken Link of Social Media Customer Service," *Social Media Today*, May 9, 2013, http://socialmediatoday.com/briansolis/1446496/first-mile-broken-link-social-media-customer-service?utm_source=feedburner&utm_medium=feed&utm_campaign=Social+Media+Today+(all+posts).

[29] "Companies Expand Their Customer Support to Include Social Media Monitoring," *Position*^{2} (blog), January 13, 2011, http://blogs.position2.com/integrating-social-media-monitoring-with-business-functions-customer-service.

[30] Drew Johnson, "GM Keeping Customers Happy Through Social Media Monitoring," *Left Lane*, March 26, 2010, www.leftlanenews.com/gm-keeping-customers-happy-through-social-media-monitoring.html.

[31] Peter Cervieri, "Dell Social Media - Linking Conversations to Sales," *ScribeMedia.org*, April 18, 2011, www.scribemedia.org/2011/04/18/dell-social-media-linking-conversations-to-sales.

[32] CATA, "About CATV," www.cata.org/About/tabid/55/Default.aspx (accessed May 10, 2013).

[33] Gabriela Saldivia, "CATA Working to Improve Customer Service Through Social Media," *Ingham County Chronicle*, February 11, 2013, http://news.jrn.msu.edu/ingham/2013/02/11/social-media-changing-customer-service-at-cata.

[34] Stuffpit, "Earn Money Recommending Products," www.stuffpit.com/stuff/earn (accessed July 2, 2011).

[35] Bob Tedeschi, "Like Shopping? Social Networking? Try Social Shopping," *New York Times*, September 11, 2006, www.nytimes.com/2006/09/11/technology/11ecom.html.

[36] Elizabeth Landau, "When Bullying Goes High Tech," CNN.com, April 15, 2013, www.cnn.com/2013/02/27/health/cyberbullying-online-bully-victims.

[37] Kate Zernike, "Son's Suicide Leads to Aid for Students," *New York Times*, February 1, 2013, www.nytimes.com/2013/02/02/nyregion/tyler-clementis-parents-work-with-rutgers-through-new-center.html?ref=cyberbullying&_r=0.

[38] Craig Giammona, "California Case Another Three-Part Tragedy of Rape, Cyber Bullying and Suicide," *NBC News*, April 14, 2013, http://usnews.nbcnews.com/_news/2013/04/14/17747411-california-case-another-three-part-tragedy-of-rape-cyber-bullying-and-suicide?lite.

[39] Rheana Murray, "Cyber-Bullying, Social Media Blamed After Florida Teen Commits Suicide," *New York Daily News*, December 12, 2012, www.nydailynews.com/news/national/social-media-blamed-teen-suicide-article-1.1218550.

[40] Jessica, "The Frightening Phenomenon of Cyberbullying," *i-lawsuit* (blog), June 6, 2013, http://cc.bingj.com/cache.aspx?q=16+states+have+passed+anti-cyberbullying+laws%2c+while+5&d=4970777129912169&mkt=en-US&setlang=en-US&w=UViNPMLI4dPUcqh-kN6uvEZt5z0FjUxU.

[41] Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D., "State Cyberbullying Laws," Cyber-Bullying Research Center, June 2011, www.cyberbullying.us/Bullying_and_Cyberbullying_Laws.pdf.

[42] Tresa Baldas, "New York Man Accused of Cyber Stalking Michigan College Students," *Detroit Free Press*, April 23, 2013, www.freep.com/article/20130423/NEWS05/304230105/college-student-cyber-stalking-naked.

[43] Kathy Tomlinson, "Teacher 'Powerless' to Stop Ex-Girlfriend's Cyberstalking," *CBC News*, May 6, 2013, www.cbc.ca/news/canada/british-columbia/story/2013/05/03/bc-cyber-stalking.html.

[44] "Cyberstalking Is a Real Crime: One in Five Americans Affected by Unwanted Contact," *PR Newswire*, January 15, 2013, www.prnewswire.com/news-releases/cyberstalking-is-a-real-crime-one-in-five-americans-affected-by-unwanted-contact-186985781.html.

[45] "State Cyberstalking and Cyberharassment Laws," National Conference of State Legislatures, November 16, 2012, www.ncsl.org/issues-research/telecom/cyberstalking-and-cyber-harassment-laws.aspx.

[46] The National Center for Victims of Crime, "Cyberstalking," www.ncvc.org/ncvc/main.aspx?dbName=DocumentViewer& Document IS=32458.

[47] Jenna Wortham, "MySpace Turns Over 90,000 Names of Registered Sex Offenders," *New York Times*, February 3, 2009, www.nytimes.com/2009/02/04/technology/internet/04myspace.html?_r=0.

[48] Brian Palmer, "There Goes the Neighborhood," *Slate*, March 22, 2013, www.slate.com/articles/business/explainer/2013/03/registered_sex_offenders_how_much_do_they_cost_their_neighbors_in_property.html.

[49] Jenna Wortham, "MySpace Turns Over 90,000 Names of Registered Sex Offenders," *New York Times*, February 3, 2009, www.nytimes.com/2009/02/04/technology/internet/04myspace.html?_r=0.

[50] Matt Smith, "Indiana Can't Kick Sex Offenders Off Social Media, Court Says," January 23, 2013, www.cnn.com/2013/01/23/tech/sex-offenders-social-media.

[51] 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.

[52] GovTrack.us, "H.R. 4472 (109th): Adam Walsh Child Protection and Safety Act of 2006," www.govtrack.us/congress/bills/109/hr4472/text (accessed July 30, 2013).

[53] GovTrack.us, "H.R. 4472 (109th): Adam Walsh Child Protection and Safety Act of 2006," www.govtrack.us/congress/bills/109/hr4472/text (accessed July 30, 2013).

[54] 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, www.gao.gov/products/GAO-13-211.

[55] Catalina Camia, "Rep. Anthony Weiner Resigns After Online Sex Scandal," *USA Today*, June 16, 2011, http://content.usatoday.com/communities/onpolitics/post/2011/06/anthony-weiner-sex-scandal-resignation-/1.

[56] Sheryl Young, "YouTube Video of Bullying Incident Gets Students Arrested," *Contributor Network*, February 4, 2011, http://news.yahoo.com/youtube-video-bullying-incident-gets-students-arrested-20110204-102400-942.html.

[57] Gene Warner, "Beating of Dog on YouTube Aids Rescue," *Buffalo News*, June 20, 2011, www.accessmylibrary.com/article-1G1-259337980/beating-dog-youtube-aids.html.

[58] Ian Lovett, "UCLA Student's Video Rant Against Asians Fuels Firestorm," *New York Times*, March 15, 2011, www.nytimes.com/2011/03/16/us/16ucla.html?_r=0.

[59] Oliver Chiang, "Meet the Man Who Just Made a Half Million from the Sale of Virtual Property," *Select Start, Forbes (blog)*, November 13, 2010, www.forbes.com/sites/oliverchiang/2010/11/13/meet-the-man-who-just-made-a-cool-half-million-from-the-sale-of-virtual-property/.

[60] Oliver J. Chiang, "The World's Most Expensive Island-Online," *Forbes*, February 17, 2010, www.forbes.com/2010/02/17/farmville-facebook-zynga-technology-business-intelligence-virtual-goods.html.

[61] Chevron, "Avatars at Chevron, Working in a Virtual World," January 21, 2011, https://id-id.facebook.com/note.php?note_id=489917545185&id=431744650466.

[62] National Highway Traffic Safety Administration, "What Is Distracted Driving?," www.distraction.gov/content/get-the-facts/facts-and-statistics.html (accessed June 24, 2013).

[63] "More Good News on the Advertiser Front – At Least Procter & Gamble Is Still Spending," *More About Advertising*, January 11, 2011, www.moreaboutadvertising.com/2011/08/more-good-news-on-the-advertiser-front-at-least-procter-gamble-is-still-spending.

[64] "Guiding Light," IMDb, www.imdb.com/title/tt0044265/ (accessed June 23, 2013).

[65] Tom Zanki, "Procter & Gamble Moves from Soap Operas to Tweets," *Lehigh Valley Express Times*, December 10, 2010, www.lehighvalleylive.com/today/index.ssf/2010/12/procter_gamble_moves_from_soap.html.

[66] Randall Stross, "Advertisers Face Hurdles on Social Networking Sites," *New York Times*, December 13, 2008, www.nytimes.com/2008/12/14/business/media/14digi.html?pagewanted=all.

[67] Alyce Lomax, "Capessa Set to Discover What Women Want," *The Motley Fool*, January 9, 2007, www.fool.com/investing/value/2007/01/09/capessa-focuses-on-women.aspx.

[68] Alyce Lomax, "Capessa Set to Discover What Women Want," *The Motley Fool*, January 9, 2007, www.fool.com/investing/value/2007/01/09/capessa-focuses-on-women.aspx.

[69] Katie Deatsch, "Procter & Gamble Sells on Facebook with Help from Amazon," *Internet Retailer*, October 1, 2010, www.internetretailer.com/2010/10/01/procter-gamble-sells-facebook-help-amazon.

[70] Tom Zanki, "Procter & Gamble Moves from Soap Operas to Tweets," *Lehigh Valley Express Times*, December 10, 2010, www.lehighvalleylive.com/today/index.ssf/2010/12/procter_gamble_moves_from_soap.html.

[71] Lauren Johnson, "Procter & Gamble Targets On-the-Go Women with Beauty App," *Mobile Marketer*, June 16, 2011, www.mobilemarketer.com/cms/news/advertising/10211.html.

[72] Tom Zanki, "Procter & Gamble Moves from Soap Operas to Tweets," Leigh Valley Express Times, December 10, 2010, www.lehighvalleylive.com/today/index.ssf/2010/12/procter_gamble_moves_from_soap.html.

[73] Susannah Fox, "Peer-to-Peer Healthcare," Pew Research Center's Internet & American Life Project, February 11, 2011, pewinternet.org/Reports/2011/P2PHealthcare.aspx, http://pewinternet.org/Reports/2011/P2PHealthcare.aspx.

[74] Claire Cain Miller, "Social Networks a Lifeline for the Chronically Ill," *New York Times*, March 24, 2010, www.nytimes.com/2010/03/25/technology/25disable.html.

[75] Alex Wilhelm, "Facebook's Stock Has Lost 31% of Its Value Since It Went Public One Year Ago," May 17, 2013, http://thenextweb.com/facebook/2013/05/17/one-year-post-ipo-facebooks-stock-is-31-under-the-level-at-which-it-went-public.

[76] Facebook, "Press Release: Facebook Reports Fourth Quarter and Full Year 2012 Results," *Yahoo! Finance*, January 30, 2013, http://finance.yahoo.com/news/facebook-reports-fourth-quarter-full-210700713.html.

[77] Facebook, "Facebook Privacy Policy," www.facebook.com/about/privacy/your-info-on-other (accessed June 21, 2013).

[78] Facebook, "Key Facts: Statistics," https://newsroom.fb.com/Key-Facts (accessed June 21, 2013).

[79] Emily Steel and Geoffrey A. Fowler, "Facebook in Privacy Breach," *Wall Street Journal*, October 18, 2010, http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html.

[80] Emily Steel and Geoffrey A. Fowler, "Facebook in Privacy Breach," *Wall Street Journal*, October 18, 2010, http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html.

[81] Daniel Ionescu, "Facebook Adds Facial Recognition to Make Photo Tagging Easier," *PCWorld*, December 16, 2010, www.pcworld.com/article/213894/facebook_adds_facial_recognition_to_make_photo_tagging_easier.html.

[82] Ed Oswald, "Facebook Facial Recognition: Security Firm Issues Alert," *PCWorld*, June 8, 2011, www.pcworld.com/article/229689/facebook_facial_recognition_security_firm_issues_alert.html.

[83] Ed Oswald, "Facebook Facial Recognition: Security Firm Issues Alert," *PCWorld*, June 8, 2011, www.pcworld.com/article/229689/facebook_facial_recognition_security_firm_issues_alert.html.

[84] Nick Bilton, "Facebook Changes Privacy Settings to Enable Facial Recognition," *Bits, New York Times* (blog), June 7, 2011, http://bits.blogs.nytimes.com/2011/06/07/facebook-changes-privacy-settings-to-enable-facial-recognition.

[85] Facebook, "Facebook and Privacy," January 31, 2013, www.facebook.com/fbprivacy/posts/532822263424357.

[86] Geoffrey A. Fowler and Christopher Lawton, "Facebook Again in Spotlight on Privacy," *Wall Street Journal*, June 8, 2011, http://online.wsj.com/article/SB10001424052702304778304576373730948200592.html.

CHAPTER 10

ETHICS OF IT ORGANIZATIONS

QUOTE

To give real service you must add something which cannot be bought or measured with money, and that is sincerity and integrity.

—Douglas Adams, English humorist and science fiction author

VIGNETTE

HP Finds Autonomy a Tough Pill to Swallow

Autonomy Corporation is a U.K. software firm whose primary product, called the Intelligent Data Operating Layer (IDOL), is marketed as an advanced search engine capable of finding information in both structured (data neatly formatted such as in spreadsheets and word documents) and unstructured form.[1]

Hewlett-Packard Company (HP) acquired Autonomy in October 2011 for $42.11 per share, a 64 percent premium over the firm's stock price. The total cost of $11 billion was 24 times Autonomy's earnings before interest payments, taxes, depreciation, and amortization (EBITDA). By way of comparison, the median price paid for 10 similar takeover deals of European software firms was 17 times EBITDA.[2,3]

Just 13 months after purchasing Autonomy, HP announced it was taking an $8.8 billion write-off related to the acquisition, Of the $8.8 billion, more than $5 billion was "linked to serious accounting

improprieties, misrepresentations and disclosure failures"[4] intended to hide the software company's true performance and value. HP alleges that such misrepresentations and lack of transparency severely affected HP's ability to perform due diligence in determining a fair value for Autonomy.[5] (**Due diligence** is the investigation of all areas of an organization prior to agreeing to a merger or other important transaction.)

Michael Lynch, founder of Autonomy, strongly denied the HP allegations. Lynch commented that he could not understand how HP could claim that the large write off was due to issues not uncovered when HP did its due diligence prior to the purchase. According to Lynch, the due diligence process involved some 300 people, including HP employees, accountants from the auditing firm KPMG, and bankers from Barclays and Perella Weinberg Partners. "It would be kind of a big elephant to have missed," Lynch said. Lynch also noted that it seemed strange that such a major problem could go unnoticed for a year and then suddenly be revealed coincident with HP announcing its worst financial results in the company's 70-year history.[6]

Deloitte, Autonomy's accounting firm prior to the acquisition, denied the HP allegations.[7] HP CEO Meg Whitman stated that as part of the due diligence process, KPMG was engaged to review the work of Deloitte and that nothing unseemly was uncovered. However, KPMG subsequently claimed that its analysis was limited strictly to a review of publicly available documents rather than a full audit of Autonomy or an examination of Deloitte's work.[8]

The U.S. Securities and Exchange Commission, the U.S. Department of Justice, and the United Kingdom's Serious Fraud Office are now investigating the situation.[9] In April 2013, HP's chairman of the board and two other board members resigned under fire from shareholders over their role in the acquisition of Autonomy.[10]

HP shareholders incensed over what now seems to have been an unreasonably high price paid for Autonomy have filed a class action lawsuit. The defendants in the lawsuit include both the current and former CEO, the former chairman of the board, several other HP senior executives, HP advisers Barclay's and Perella Weinberg, and Autonomy's founder Lynch. The shareholders allege that HP overlooked numerous issues concerning Autonomy's financial condition and accounting irregularities.[11]

Questions to Consider

1. If Autonomy management used accounting shenanigans to make the firm look more attractive to HP and HP was unable to discern these tricks, should the Autonomy management team be viewed in a positive light by the original Autonomy shareholders who earned a 64 percent premium on their shares? Why or why not?
2. What is your evaluation of HP senior management in relation to the acquisition of Autonomy? Should the HP team be held accountable if Autonomy management duped them?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What are contingent workers, and how are these workers employed in the information technology industry?
2. What key ethical issues are associated with the use of contingent workers, including H-1B visa holders and offshore outsourcing companies?
3. What is whistle-blowing, and what ethical issues are associated with it?
4. What is an effective whistle-blowing process?
5. What measures are members of the electronics manufacturing industry taking to ensure the ethical behavior of the many participants in their long and complex supply chains?
6. What is green computing, and what are organizations doing to support this initiative?

KEY ETHICAL ISSUES FOR ORGANIZATIONS

This chapter touches on the following ethical topics that are pertinent to organizations in the IT industry, as well as to organizations that make use of IT:

- The use of nontraditional workers, including temporary workers, contractors, consulting firms, H-1B visa workers, and outsourced offshore workers, gives an organization more flexibility in meeting its staffing needs, often at a lower cost

than if the organization used traditional workers. The use of nontraditional workers also raises ethical issues for organizations. When should such nontraditional workers be employed, and how does such employment affect an organization's ability to grow and develop its own employees? How does the use of nontraditional workers impact the wages of the organization's own employees?

- Whistle-blowing, as discussed in Chapter 2, is an effort to attract public attention to a negligent, illegal, unethical, abusive, or dangerous act by a company or some other organization. It is an important ethical issue for individuals and organizations. How can you safely and effectively report misconduct, and how should managers handle a whistle-blowing incident?
- **Green computing** is a term applied to a variety of efforts directed toward the efficient design, manufacture, operation, and disposal of IT-related products, including personal computers, laptops, servers, printers, and printer supplies. Computer manufacturers and end users are faced with many questions about when and how to transition to green computing, and at what cost.
- The electronics and information and communications technology (ICT) industry recognizes the need for a code to address ethical issues in the areas of worker safety and fairness, environmental responsibility, and business efficiency. What has been done so far, and what still needs to be done?

Let's begin with a discussion of the use of nontraditional workers and the ethical issues raised by this practice.

The Need for Nontraditional Workers

According to the Computing Research Association, the number of undergraduate degrees awarded in computer science, computer engineering, and information technology at doctoral-granting computer science departments in the United States and Canada decreased dramatically from a peak of around 21,000 per year in 2004 to less than 10,000 in 2009.[12] By 2011, however, the number of undergraduate degrees had rebounded to nearly 15,000 (see Figure 10-1). This recovery was due in part to the federal government's forecast of an increased need for workers in computer science-related fields.

The Bureau of Labor Statistics estimates that as of 2010, there were 3.4 million people employed in IT-related positions in the United States; the agency expects this sector to add close to 750,000 new jobs between 2010 and 2020.[13] Figure 10-2 shows the total number of people needed for selected IT positions as well as the median 2010 salaries associated with these positions.

As a result of the decline in undergraduate degrees being awarded in computer science and engineering fields, IT firms and organizations that use IT products and services are concerned about a shortfall in the number of U.S. workers to fill not only the 750,000 expected new positions but also to replace the many people who will retire from existing positions. Facing a likely long-term shortage of trained and experienced workers, employers are increasingly turning to nontraditional sources to find IT workers with skills that meet their needs; these sources include contingent workers, H-1B workers, and outsourced offshore workers. As employers consider these options, they must confront ethical decisions about whether to recruit new and more skilled workers from these sources or to develop their own staff to meet the needs of their business.

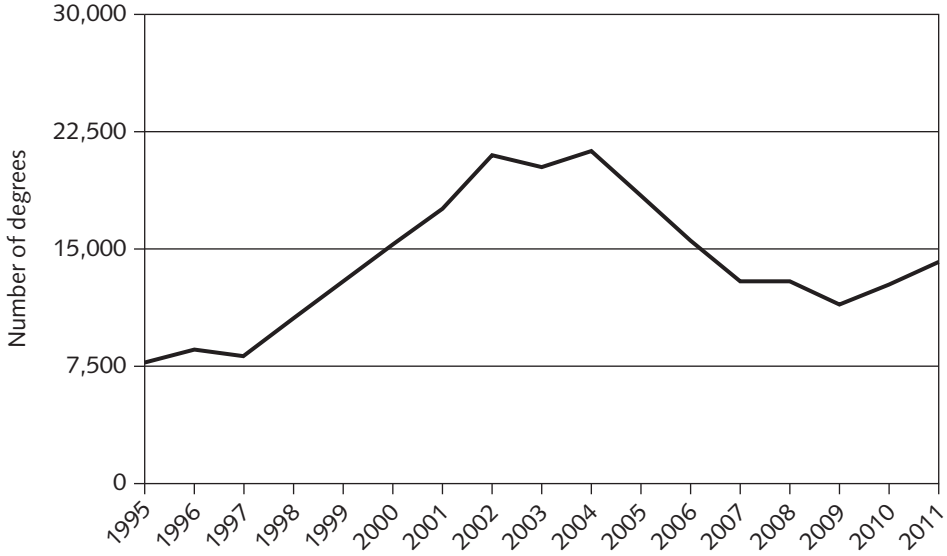


FIGURE 10-1 Number of undergraduate degrees awarded in computer science, computer engineering, and information systems

Source Line: CRA Taulbee Survey; Computing Degree and Enrollment Trends 2010-2011.

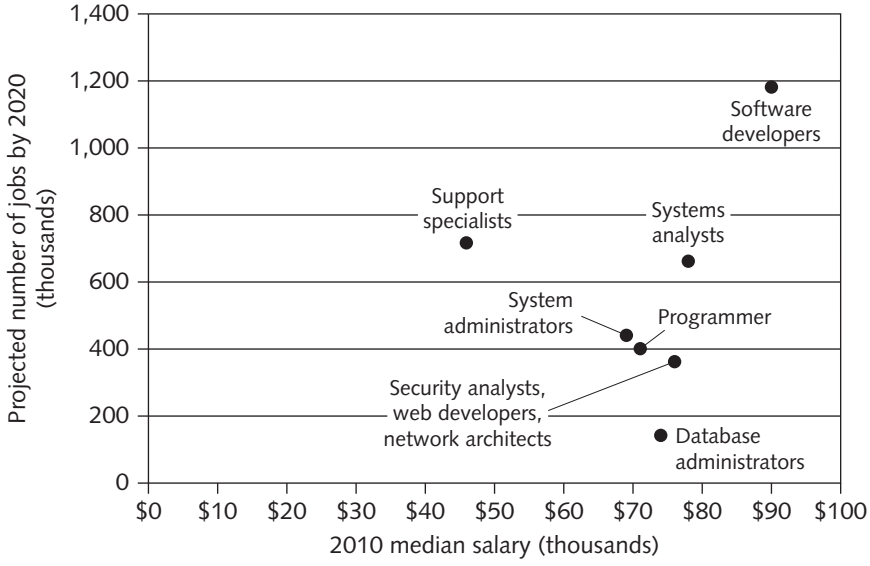


FIGURE 10-2 Occupational outlook, IT positions

Source Line: Occupational Outlook Handbook, www.bls.gov/ooh/computer-and-information-technology/software-developers.htm (accessed June 8, 2013).

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. The contingent workforce includes independent contractors, temporary workers hired through employment agencies, on-call or day laborers, and on-site workers whose services are provided through contract firms.

A firm is likely to use contingent IT workers if it experiences pronounced fluctuations in its technical staffing needs. Workers are often hired on a contingent basis 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 new information systems.

Typically, these workers join a 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 or employee leasing 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. 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 considered official employees of the company, so they are not eligible for company benefits such as vacation, sick pay, and medical insurance. Because temporary workers do not receive additional compensation through company benefits, they are often paid a higher hourly wage than full-time employees doing equivalent work. Temporary working arrangements sometimes appeal to people who want maximum flexibility in their work schedule as well as a variety of work experiences. Other workers take temporary work assignments only 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 firms operate with minimal administrative, sales, and marketing staff to keep down overall costs, and they pass the savings on to their clients. Employee leasing is a type of **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 firm. Organizations can also obtain temporary IT employees by hiring a consulting firm. Consulting organizations maintain a staff of employees with a wide range of skills and experience, up to and including world-renowned industry experts; thus, these firms can often provide the exact skills and expertise that an organization requires for a particular project. Consulting firms work with their clients on engagements for which there are typically well-defined expected results or deliverables that must be produced (e.g., creation of an IT strategic plan, implementation of an enterprise resource planning [ERP] system, or

selection of a hardware vendor). The contract with a consulting firm typically specifies the length of the engagement and the rate of pay for each of the consultants, who are directed on the engagement by a senior manager or director from the consulting firm. Table 10-1 shows the world's largest IT consulting firms (in alphabetical order). Each of these firms has over 100,000 employees.

TABLE 10-1 Large IT consulting firms

Firm	Headquarters
Accenture	Dublin, Ireland
Cognizant Technology Solutions	Teaneck, New Jersey
Capgemini	Paris, France
Deloitte Touche Tohmatsu	New York, New York
Ernst & Young	New York, New York
HP Enterprise Business	Palo Alto, CA
IBM Global Business Services	Armonk, New York
Infosys	Bangalore, India
KPMG	Amstelveen, Netherlands
Tata Consultancy Services	Mumbai, India
Wipro Technologies	Bangalore, India

Source Line: Course Technology/Cengage Learning.

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 they 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 customers 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.

For example, in 2001, Microsoft agreed to pay a $97 million settlement to some 10,000 "permatemps"—temporary workers who were employed for an extended length of time as software testers, graphic designers, editors, technical writers, receptionists, and office support staffers. Some had worked at Microsoft for several years. The *Vizcaino v. Microsoft* class action was filed in 1992 by eight former workers who claimed that they—and thousands of other permatemps—had been illegally shut out of a stock purchase plan that allowed employees to buy Microsoft stock at a 15 percent discount. Microsoft shares had skyrocketed in value throughout the 1990s. The sharp appreciation in the stock price meant that had they been eligible, some temporary workers in the lawsuit could have earned more money from stock gains than they received in salary while at Microsoft.[14]

The *Vizcaino v. Microsoft* lawsuit dramatically illustrated the cost of misclassifying employees and violating laws that cover compensation, taxes, unemployment insurance, and overtime. The key lesson of this case is that even if workers sign an agreement indicating that they are contractors and not employees, the deciding factor is not the agreement but the degree of control the company exercises over the employees. The following questions can help determine whether a worker is an employee:

- Does the worker have the right to control the manner and means of accomplishing the desired result?
- How much work experience does the person have?
- Does the worker provide his own tools and equipment?
- Is the worker engaged in a distinct occupation or an independently established business?

- Is the method of payment by the hour or by the job?
- What degree of skill is required to complete the job?
- Does the worker hire employees to help?

The Microsoft ruling means that employers must exercise care in their treatment of contingent workers. If a company wants to hire contingent workers through an agency, then the agency must hire and fire the workers, promote and discipline them, do performance reviews, decide wages, and tell them what to do on a daily basis.

Read the manager's checklist in Table 10-2 for questions that pertain to the use of contingent workers. The preferred answer to each question is *yes*.

TABLE 10-2 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 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?		
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?		

Source Line: Course Technology/Cengage Learning.

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. Many companies turn to H-1B workers to meet critical business needs or to obtain essential technical skills and 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. Employers often need H-1B

professionals to provide special expertise in overseas markets or on projects that enable U.S. businesses to compete globally. A key requirement for using H-1B workers is that employers must pay H-1B workers the prevailing wage for the work being performed.

A person can work for a U.S. employer as an H-1B employee for a maximum continuous period of six years. With sponsorship from their employers, H-1B visa holders can apply for permanent residence. During the application periods, their H-1B visas can be renewed in one-year extensions until their green card is issued. Should a worker's H-1B visa expire, the foreign worker must remain outside the United States for one year before another H-1B petition will be approved.[15] Table 10-3 shows the employers who received approval for the most H-1B visas in 2012.

TABLE 10-3 Top H-1B visa employers in 2012

Company	Total H-1B visas granted (2012)
Cognizant	9,281
Tata	7,469
Infosys	5,600
Wipro	4,304
Accenture	4,037
HCL America	2,070
Tech Mahindra SATYAM	1,963
IBM & IBM India	1,846
Larsen & Toubro	1,632
Deloitte Touche Tohmatsu	1,668

Source Line: Ron Hira, "Top 10 Users of H-1B Guest Workers Program Are All Offshore Outsourcing Firms," Economic Policy Institute (blog), February 14, 2013, www.epi.org/blog/top-10-h1b-guestworker-offshore-outsourcing.

The top five countries of birth for H-1B workers in 2011 were India with 58 percent of all approved H-1B petitions, China (9%), Canada (4%), the Philippines (3%), and South Korea (3%).[16]

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 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. Roughly 50 percent of all 2012 H-1B recipients were in IT-related occupations.[17]

When considering the use of H-1B visa workers, companies should take into account that even highly skilled and experienced H-1B workers may require help with their

English skills. Communication in many business settings is fast paced and full of idiomatic expressions; workers who are not fluent in English may find it difficult and uncomfortable to participate. As a result, some H-1B workers might become isolated. Even worse, H-1B workers who are not comfortable with English may gradually stop trying to acclimate and may create their own cliques, which can hurt a project team's morale and lead to division. Managers and coworkers should make it a priority to assist H-1B workers looking to improve their English skills and to develop beneficial working relationships based on a mutual respect for any cultural differences that may exist. H-1B workers must feel at ease and be able to interact easily and feel like true members of their team.

Even as concern increases about the ability to fill job openings, some in the IT sector—including displaced workers and other critics—challenge whether the United States needs to continue importing thousands of H-1B workers every year. Many business managers, however, say such criticisms conceal the real issue, which is the struggle to find qualified people, wherever they are, for increasingly challenging work. Heads of many U.S. companies complain that they have trouble finding enough qualified IT employees and have urged the USCIS to loosen the reins on visas for qualified workers. Some human resource managers and educators are concerned that the continued use of H-1B workers may be a symptom of a larger, more fundamental problem—that the United States is not developing a sufficient number of IT employees with the right skills to meet its corporate needs.

Many IT workers in the United States have expressed concern that the use of H-1B workers has a negative impact on their wages. Researchers from New York University and the Wharton School of the University of Pennsylvania examined tens of thousands of resumes as well as demographic and wage data on 156,000 IT workers employed at 7,500 publicly held U.S. firms. Their conclusion was that "H-1B admissions at current levels are associated with a 5 percent to 6 percent drop in wages for computer programmers, systems analysts, and software engineers." The researchers also concluded that "there is substantial evidence that H-1B admissions appear to directly improve levels of innovation and entrepreneurship, which in the long term should create new jobs and raise demand for technology workers in other areas.[18]

Meanwhile, many observers believe that reducing the number of foreign nationals that U.S. firms may hire to work inside the United States will have the negative effect of encouraging these firms to open offices to place these workers outside the United States. Such action would lessen growth and investment in the United States.[19]

H-1B Application Process

Most companies make ethical hiring decisions based on how well an applicant fulfills the job qualifications. Such companies consider the need to obtain an H-1B visa *after* deciding to hire the best available candidate. To receive an H-1B visa, the person must have a job offer from an employer who is also willing to offer sponsorship.

Once a decision has been made to hire a worker who will require an H-1B visa, an employer must begin the application process. There are two application stages: the Labor Condition Application (LCA) and the H-1B visa application. The company files an LCA with the Department of Labor (DOL), stating the job title, the geographic area in which the worker is needed, as well as the salary to be paid. The DOL's Wage and Hour Division reviews the LCA to ensure that the foreign worker's wages will not undercut those of an

American worker. After the LCA is certified, the employer may then apply to the USCIS for the H-1B visa, identifying who will fill the position and stating the person's skills and qualifications for the job. A candidate cannot be hired until the USCIS has processed the application, which can take several days or several months.[20]

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 their current U.S. workers? Heavy reliance on the use of H-1B workers can lessen the incentive for U.S. companies to educate and develop their own workforces.

Potential Exploitation of H-1B Workers

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 greatly, 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. Unethical companies can also find other ways to get around the salary protections included in the H-1B program, as shown in the charges filed against Vision Systems Group. In 2009, the company was charged with H-1B visa fraud for allegedly stating that certain H-1B workers in its New Jersey office were actually working in Iowa, where the company had another office and where the prevailing wage is much less. The president and another officer of the firm were sentenced to three years' probation, and the company was forced to pay $236,250 to the U.S. Citizenship and Immigration Services.[21]

Until Congress approved the Visa Reform Act of 2004, there were few investigations into H-1B salary abuses. The act increased the H-1B application fee by $2,000, of which $500 was earmarked for antifraud efforts; the act also defined a modified wage-rate system, allowing for greater variances in pay to visa holders. Investigations are typically triggered by complaints from H-1B holders, but the government can conduct random audits or launch an investigation based on information from third-party sources.

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.

Unethical employers may lie on their H-1B applications to take advantage of the program. For instance, six top executives of Dibon Solutions, an IT consulting firm, were arrested on charges of H-1B visa fraud and related wire fraud. The conspirators recruited and sponsored foreign IT workers, indicating on their visa applications that the workers would be paid an annual salary to work full-time at Dibon headquarters in Carrollton,

Texas. (These conditions were required to obtain the visas.) However, the foreign workers were actually placed at various third-party companies, and were only paid if the third-party company first paid Dibon for its services. This ruse provided Dibon with a large pool of inexpensive labor that could be used on an "as-needed" basis.[22]

OUTSOURCING

Outsourcing is another approach to 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, or staffing a computer help desk.

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.

In the 1970s, IT executives started the trend toward outsourcing as they began to supplement their IT staff with contractors and consultants. This trend eventually led to companies outsourcing entire IT business units to organizations such as Accenture, Electronic Data Systems, and IBM—which could take over the operation of a company's data center as well as perform other IT functions.

Offshore Outsourcing

Offshore outsourcing is a form of outsourcing in which the 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, offshore outsourcing occurs frequently in the IT field. A 2010 survey indicated that 93 percent of multinational companies had undertaken some sort of IT outsourcing project.[23] American Express, Aetna, Compaq, General Electric, IBM, Microsoft, Motorola, Shell, Sprint, and 3M are examples of big companies that employ offshore outsourcing for functions such as help-desk support, network management, and information systems development.

As more businesses move their key processes offshore, U.S. IT service providers are forced to lower prices. 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 facilities in Canada, Great Britain, 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. According to the Gartner Group, some of the top sources of contract programming include Argentina, Australia, Belarus, Brazil, Bulgaria, Canada, China, India, Ireland, Israel, Malaysia, Malta, Mexico, Nepal, the Philippines, Poland, Russia, Serbia, Singapore, Sri Lanka, and Vietnam.[24] 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.

Organizations must consider many factors when deciding where to locate outsourcing activities. For example, political unrest in Egypt has 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.[25] Global management consulting firm A.T. Kearney publishes the Global Services Location Index, which ranks the 50 most attractive offshoring destinations based on 39 measures across three primary categories: financial attractiveness, people and skills availability, and overall business environment. Table 10-4 lists the top ten countries from the index's 2011 rankings.

TABLE 10-4 Most attractive offshoring destinations (based on A.T. Kearney rating methodology)

Country
1. India
2. China
3. Malaysia
4. Egypt
5. Indonesia
6. Mexico
7. Thailand
8. Vietnam
9. Philippines
10. Chile

Source Line: A.T. Kearney, Inc., "A.T. Kearney's Global Services Location Index™," © 2011, www.atkearney.com/index.php/Publications/at-kearneys-global-services-location-index-volume-xiii-number-2-2010.html.

In 2011, Nokia, the Finnish mobile device manufacturer, and Accenture, the global consulting company headquartered in Ireland, announced a major outsourcing deal in which Accenture agreed to provide Nokia with software development and support services for the once popular Symbian mobile operating system and computing platform. Some 2,300 Nokia employees in China, Denmark, Finland, India, the United Kingdom, and the United States were transferred to Accenture as part of the deal. Symbian has fallen out of favor with phone handset manufacturers, and Nokia has decided to transition to a Windows Phone platform for its line of smartphones. As part of the outsourcing agreement, Accenture became the preferred supplier to Nokia to aid its transition from Symbian to the Windows Phone platform.[26]

Table 10-5 lists the top IT outsourcing firms according to the International Association of Outsourcing Professionals.

TABLE 10-5 Top-rated IT outsourcing firms according to the International Association of Outsourcing Professionals

Firm	Headquarters location
Accenture	Dublin, Ireland
Wipro Technologies	Bangalore, India
Infosys Technologies	Bangalore, India
HCL Technologies	New Delhi, India
CSC	Falls Church, Virginia
Capgemini	Paris, France
Amdocs	Chesterfield, Missouri
CGI Group	Montreal, Quebec, Canada

Source Line: International Association of Outsourcing Professionals, "The 2013 Global Outsourcing 100," © 2013, www.iaop.org/Content/19/165/3612.

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, the state of New Mexico contracted the development of a tax 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. 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 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. For example, Dex One Corporation, whose products include yellow pages print directories and an online ad network, outsourced much of its IT work to HGL Technologies to speed up development of new digital offerings while simultaneously cutting operational costs. As a result of this deal, about 30 percent of the Dex One IT staff was eliminated.[27] Offshore outsourcing tends to upset domestic staff when a company begins to lay off employees in favor of low-wage workers outside the United States. The remaining members of a department may become bitter and nonproductive, and morale may be affected.

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. For example, Atlanta's Grady Memorial Hospital discovered that 45 patient records—including doctors' notes, diagnoses, and medical conditions—were accessible on an unsecured, publicly available Web site for a few weeks due to an error by an outsourcing firm in India. The hospital had outsourced the job of transcribing patient records to a Georgia firm, which outsourced it to a Nevada contractor, which in turn outsourced the job to the company in India.[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 state-of-the-art telecommunications setup
- High-quality on-site managers and supervisors

To ensure that company data is protected in an outsourcing arrangement, companies can use the Statement on Auditing Standards (SAS) No. 70, Service Organizations, an internationally recognized standard developed by the American Institute of Certified Public Accountants (AICPA). A successful SAS No. 70 audit report demonstrates that an outsourcing firm has effective internal controls in accordance with the Sarbanes-Oxley Act of 2002.

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 SAS No. 70 audit report to ascertain its level of control over information technology and related processes.

WHISTLE-BLOWING

Like the subject of contingent workers, whistle-blowing is a significant topic in any discussion of ethics in IT. Both issues raise ethical questions and have social and economic implications. How these issues are addressed can have a long-lasting impact not only on the people and employers involved, but also on the entire IT industry.

As noted previously, 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. 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.

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. During 2012, the United States Department of Justice recovered $4.9 billion in false claim cases involving fraud against the government.[29]

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.[30]

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.[31] 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.[32]

In a lawsuit initially brought by a whistle-blower in 2007 and settled in 2011, Verizon agreed to pay the federal government $93.5 million due to allegations that the company had overcharged the federal government on voice and data communications contracts for years. The whistle-blower alleged Verizon had billed the government for "tax-like" surcharges to which the government was not subject.[33] In this case, the government refused to pay the whistle-blower the statutory minimum amount of 15 percent ($14 million) because it disputed "the extent to which the relater 'substantially contributed' to the $93.5 million settlement between Verizon and the United States." Instead the whistle-blower was awarded just $4 million, an amount he challenged in court.[34]

An Oracle shareholder sued the company's board of directors—including CEO Larry Ellison—for alleged "gross mismanagement" of their handling of a False Claims lawsuit involving the firm. The shareholder contends that the Board should have simply admitted that Oracle had committed a crime, implemented necessary safeguards to ensure it would not happen again, and negotiated a relatively small fine. Instead, the shareholder claims, Oracle took action to fight the lawsuit, which resulted in Oracle being forced to settle with the government for the sum of $200 million. The original False Claims lawsuit was brought because Oracle influenced the General Services Administration to buy over $1 billion in software by falsely guaranteeing that the government would receive the same discounts that the company offered its favored customers.[35]

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.[36]

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.

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 their source.[37]

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 continuing to work 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 air or 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, and 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.[38] 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, *http://sla.ckers.org*. In the forum, he revealed serious security weaknesses in 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.[39] This is a perfect example of how *not* to be a whistle-blower.

GREEN COMPUTING

Many computer manufacturers today are talking about building a "green PC," by which they usually mean one that uses less electricity to run than the standard computer; thus, its carbon footprint on the planet is smaller. However, to manufacture a truly green PC, a hardware company must also reduce the amount of hazardous materials and dramatically increase the amount of reusable or recyclable materials used in its manufacturing and packaging processes. The manufacturers must also help consumers dispose of their products in an environmentally safe manner at the end of their useful life.

Electronic devices such as personal computers and cell phones contain hundreds or even thousands of components. The components, in turn, are composed of many different materials, including some that are known to be potentially harmful to humans and the environment, such as beryllium, cadmium, lead, mercury, brominated flame retardants (BFRs), selenium, and polyvinyl chloride.[40]

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. The United States has no federal law prohibiting the export of toxic waste, so many used electronic devices intended for recycling are sold to companies in developing countries that try to repair the components or extract valuable metals from them, using methods that release carcinogens and other toxins into the air and the water supply.[41]

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).[42] Individual purchasers as well as corporate purchasers of computers, printers, scanners, and multifunction devices can use the EPEAT Web site (*www.epeat.net)* to screen manufacturers and models based on environmental attributes.[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]

It is estimated that 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 the United States in 2010.[45] How should users safely dispose of their obsolete computers? Over half the states have established statewide programs for some recycling of obsolete computers. These statutes either impose a fee for each unit sold at retail or require manufacturers to reclaim the equipment at disposal.[46]

Some electronics manufacturers have developed programs to assist their customers in disposing of old equipment. For example, Dell offers a free worldwide recycling program for consumers. It also provides no-charge recycling of any brand of used computer or printer with the purchase of a new Dell computer or printer. This equipment is recycled in an environmentally responsible manner, using Dell's stringent global recycling guidelines.[47] HP and other manufacturers offer similar programs.

The environmental activist organization Greenpeace issues ratings of the top manufacturers of personal computers, mobile phones, TVs, and game consoles based on the manufacturers' policies on toxic chemicals, recycling, and climate change. Table 10-6 shows the companies with the top ten Greenpeace ratings in November 2012. With 10 being a perfect score, it is clear that these manufacturers have a long way to go in meeting the very high "green" standards of Greenpeace.

TABLE 10-6 Greenpeace ratings of the top ten electronics manufacturers

Organization	October 2012 rating
Wipro	7.1
Hewlett Packard	5.7
Nokia	5.4
Acer	5.1
Dell	4.6
Apple	4.5
Samsung	4.2
Sony	4.1
Lenovo	3.9
Phillips	3.8

Source Line: Greenpeace, "Guide to Greener Electronics," © November 2012, www.greenpeace.org/international/en/Guide-to-Greener-Electronics/18th-Edition.

ICT INDUSTRY CODE OF CONDUCT

The **Electronic Industry Citizenship Coalition (EICC)** was established to promote a common code of conduct for the electronics and ICT industry.[48] The EICC focuses on the areas of worker safety and fairness, environmental responsibility, and business efficiency. ICT organizations, electronics manufacturers, software firms, and manufacturing service providers may voluntarily join the coalition.

The EICC has established a code of conduct that defines performance, compliance, auditing, and reporting guidelines across five areas of social responsibility: labor, health and safety, environment, management system, and ethics. Adopting organizations apply the code across their entire worldwide supply chain and require their first-tier suppliers to acknowledge and implement it.[49] As of June 2013, the code has been formally adopted by over 86 EICC member organizations, including Apple, Cisco, Dell, HP, IBM, Intel, Lenovo, Microsoft, Oracle, Samsung, and Sony. The following are the five areas of social responsibility and guiding principles covered by the code:[50]

1. *Labor*—"Participants are committed to uphold the human rights of workers, and to treat them with dignity and respect as understood by the international community."

2. *Health and Safety*—"Participants recognize that in addition to minimizing the incidence of work-related injury and illness, a safe and healthy work environment enhances the quality of products and services, consistency of production and worker retention and morale. Participants also recognize that ongoing worker input and education is essential to identifying and solving health and safety issues in the workplace."
3. *Environmental*—"Participants recognize that environmental responsibility is integral to producing world class products. In manufacturing operations, adverse effects on the community, environment, and natural resources are to be minimized while safeguarding the health and safety of the public."
4. *Management System*—"Participants shall adopt or establish a management system whose scope is related to the content of this Code. The management system shall be designed to ensure (a) compliance with applicable laws, regulations and customer requirements related to the participant's operations and products; (b) conformance with this Code; and (c) identification and mitigation of operational risks related to this Code. It should also facilitate continual improvement."
5. *Ethics*—"To meet social responsibilities and to achieve success in the marketplace, participants and their agents are to uphold the highest standards of ethics including: business integrity; no improper advantage; disclosure of information; intellectual property; fair business, advertising, and competition; protection of identity; responsible sourcing of minerals; and privacy."

Prior to the adoption of the EICC Code of Conduct, many electronic manufacturing companies developed their own codes of conduct and used them to audit their suppliers. Thus, suppliers could be subjected to multiple, independent audits based on different criteria. The adoption of a single, global code of conduct by members of the EICC enables those companies to provide leadership in the area of corporate social responsibility. It also exerts pressure on suppliers to meet a common set of social principles.

The EICC has developed an audit program for member organizations in which audits are conducted by certified, third-party audit firms. EICC members use the audits to measure supplier compliance with the EICC Code of Conduct and to identify areas for improvement.

Summary

- IT firms and organizations that use IT products and services are concerned about a shortfall in the number of U.S. workers to fill these positions. As a result, they are turning to nontraditional sources to find IT workers with skills that meet their needs.
- Contingent work is a job situation in which an individual does not have an explicit or implicit contract for long-term employment. The contingent workforce includes independent contractors, temporary workers hired through employment agencies, on-call or day laborers, and on-site workers whose services are provided through contract firms.
- 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.
- Some people contend that employers exploit contingent workers, especially H-1B foreign workers, to obtain skilled labor at less-than-competitive salaries. Others believe that the use of H-1B workers is required to keep the United States competitive.
- Employers must make ethical decisions about whether to recruit new and more skilled workers from these sources or to spend the time and money to develop their current staff to meet the needs of their business.
- 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.
- 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.
- 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.

- Computer companies looking to manufacture green computers are challenged to produce computers that use less electricity, include fewer hazardous materials that may harm people or pollute the environment, and contain a high percentage of reusable or recyclable material. These companies should also provide programs to help consumers dispose of their products in an environmentally safe manner at the end of their useful life.
- EPEAT (Electronic Product Environmental Assessment Tool) 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.
- The Electronic Industry Citizenship Coalition (EICC) has established a code of conduct that defines performance, compliance, auditing, and reporting guidelines across five areas of social responsibility: labor, health and safety, environment, management system, and ethics.
- A number of electronics manufacturers have applied this code across their entire worldwide supply chain and also require their first-tier suppliers to acknowledge and implement the code.

Key Terms

coemployment relationship
contingent work
due diligence
Electronic Industry Citizenship Coalition (EICC)
Electronic Product Environmental Assessment Tool (EPEAT)
employee leasing
False Claims Act
green computing
H-1B visa
offshore outsourcing
outsourcing
qui tam

Self-Assessment Questions

The answers to the Self-Assessment Questions can be found in Appendix B.

1. The IT position with the highest 2010 median salary is:
   a. system administrator
   b. programmer
   c. database administrator
   d. software developer

2. Which of the following statements is true about future job prospects in the IT industry?
   a. The Bureau of Labor Statistics estimates that as of 2010, 3.4 million people were employed in IT-related positions in the United States, and the agency expects this sector to add around 750,000 new jobs between 2010 and 2020.
   b. After several years of increasing, the number of undergraduate degrees granted in computer science, computer engineering, and information systems is now declining.
   c. U.S. employers should have no problem recruiting IT workers with the skills that meet their needs.
   d. None of the above
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. Depending on how closely workers are supervised and how the job is structured, contingent workers can be viewed as permanent employees by the IRS, the U.S. Department of Labor, or a state's workers' compensation and unemployment agencies. True or False?
5. A temporary working visa granted by the U.S. Citizenship and Immigration Services 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—is called a (an) _____ visa.
6. Which of the following countries was the top country of birth for H-1B workers in the United States in 2011?
   a. Canada
   b. Mexico
   c. China
   d. India
7. Many observers believe that reducing the number of foreign nationals that U.S. firms hire would lessen growth and investment in the United States. True or False?
8. According to A.T. Kearney, the three most attractive offshoring destinations are:
   a. India, Egypt, and Philippines
   b. India, China, and Malaysia
   c. Vietnam, Philippines, and Chile
   d. China, Mexico, and Thailand
9. The cost advantage for Indian workers over U.S. workers continues to increase. True or False?

10. 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. Whistle-blowing is an effective approach to take in dealing with all work-related matters, from the serious to mundane.
    c. 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.
    d. A whistle-blower must be an employee of the company that is the source of the problem.
11. Which of the following are desirable characteristics of a "green computer"?
    a. It runs on less electricity than the typical computer.
    b. It contains a high percentage of reusable or recyclable materials.
    c. Its manufacturer has a program to help consumers dispose of it at the end of its life.
    d. All of the above
12. It is estimated that over 1 million tons of computers, monitors, and hard copy devices were disposed of in the United States in 2010. True or False?
13. _____ was the highest-ranked manufacturer by Greenpeace for its excellent corporate policies in regard to toxic chemicals, recycling, and climate change in 2012.
14. Products are ranked in EPEAT according to three tiers of environmental performance, with _____ being the highest.

Discussion Questions

1. Edward Snowden—an employee of defense contractor Booz Allen Hamilton, working at the National Security Agency (NSA)—is responsible for what may turn out to be 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 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 paper explaining your point of view on Snowden.
2. During a time in which unemployment in the United States exceeds 7 percent, 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. What set of reasons is stronger? Why?
3. Wipro received the highest rating of electronics manufacturers from Greenpeace for its efforts in green computing. Visit Wipro's Web site, and document several examples of the company efforts to improve its green computing results.

4. What factors must a company consider in deciding whether to employ offshore outsourcing on a project?
5. Visit the EPEAT Web site (*www.epeat.net*), and use the organization's tool to select your next laptop 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?
6. You work for an electronics manufacturer that does not belong to the EICC. Present a strong argument for your firm to join. Then present a strong argument for why it makes sense for your firm not to be a member.
7. Although labor savings associated with offshore outsourcing may look attractive, what cost increases and other problems can you expect with such projects?
8. Why do companies that make use of a lot of contingent workers fear getting involved in a coemployment situation? What steps should they take to avoid this situation?

9. 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?
10. 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?

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 an entry-level worker in the audit department of the Internal Revenue Service, and you have stumbled across evidence of a program to turn off the audit process for major contributors to the current president's reelection campaign. In effect, select taxpayers can make any claim on their tax returns without fear of being audited or investigated. What would you do?
2. A coworker complains to you that he is sick of seeing the company 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 do?
3. 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 challenged 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 outsourcing work. What advice would you offer your friend?

4. 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 you to 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? What would you do?
5. 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 Web site (*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?
6. 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 1,200 new laptops to deploy to the worldwide salesforce. 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?
7. You are the manager of a large IT project that will involve two dozen offshore outsourced workers who will do program development and testing. Identify several potential issues that could arise on this project due to the outsourcing arrangement. What specific steps would you take to improve the likelihood of success of the project?
8. Your firm relies heavily on temporary workers. To minimize potential legal issues, it ensures that the temporary workers are not mistaken about their place within the company. Therefore, temporary employment agencies provide these workers with a handbook

that lays out the ground rules in explicit detail. Temporary workers are barred from using company-owned athletic fields—for insurance reasons, the handbook explains. Temporary workers are told not to park their cars in the company parking lot because it would create parking problems for regular workers. Temporary workers are also told not to buy goods at the company store, eat in the company cafeteria, or participate in company social clubs such as chess, tai chi, or line dancing, which are open to regular employees. They are not permitted to attend parties given for regular employees, company-sponsored screenings of the latest movies, or company meetings that are often held at the local convention center. In addition, their email addresses must contain an n- prefix to indicate their non-permanent status in the company.

Imagine that you are a newly hired manager in the Human Resources Department and that you have been asked to respond to complaints from several temporary workers about working conditions. What sort of complaints would you expect to hear? How would you handle this?

9. Catalytic Software—a U.S.-based IT outsourcing firm with offices in both Redmond, Washington, and Hyderabad, India—wants to tap India's large supply of engineers as contract software developers for IT projects. However, instead of just outsourcing projects to local Indian software development companies, as is the common practice of U.S. companies, Catalytic has developed a self-contained company community near Hyderabad. Spread over 500 acres, the community of New Oroville is a self-sustaining residential and office community designed to house about 4,000 software developers and their families, as well as 300 support personnel who supply sanitation, police, and fire services.

   The goal of this high-tech city is to knock down barriers that large-scale technology businesses encounter in India. By building a company community, Catalytic is trying to ensure that it has enough qualified employees to staff around-the-clock shifts. The company expects this facility to attract and keep top professionals from all over the world. Building a company town also solved the problem of transportation, which can be challenging for such a large workforce. Because of the terrible state of the local roads, the commute from Hyderabad—25 kilometers from New Oroville—would take almost an hour.

   Catalytic provides private homes with private gardens, all within a short walk of work, school, recreation, shopping, and public facilities. Each house includes cable television, telephones, and a fiber-optic data pipeline that connects to the Internet so that employees can work efficiently even at home. (Employees are awarded bonuses for working overtime.) New Oroville was designed to include four indoor recreational complexes, six large retail complexes, and ample green space, including five parks for outdoor exercise and recreation.

   You have just completed a job interview with Catalytic Software for a position as project manager and have been offered a 25 percent raise to join the company. Your position will be based in Redmond and will involve managing U.S.-based projects for customers. The position requires that you spend the first year with Catalytic in the New Oroville facility to learn its methods, culture, and people. (You can take your entire family or accept a pair of three-week company-paid trips back to Redmond.)

   Why do you think the temporary assignment in New Oroville is a requirement? What else would you need to know in considering this position? Would you accept it? Why or why not?

Cases

1. IBM Provides Supply Chain Leadership

In 2013, the U.S. Environmental Protection Agency (EPA) presented IBM with a Climate Leadership Award.[51] IBM has served as an environmental steward "during periods when the environment was not always as popular a subject as it is today; during profound changes in the global economy, our industry, and our business model; and during periods of differing financial results," notes Wayne S. IBM's Vice President for Corporate Environmental Affairs and Product Safety.[52] IBM is publicly committed to making its products environmentally friendly, energy efficient, reusable, recyclable, and safely disposable. As an IT giant, IBM significantly impacts environmental health by reducing its own environmental footprint.

The EPA recognized IBM because of its ambitious emissions reduction goals and because it has become a supply chain leader, requiring that companies up and down its supply chain establish environmental sustainability programs. At first, this may not seem impressive, as many of IBM's suppliers are much smaller companies with smaller carbon footprints. However, IBM has over 27,000 suppliers, ranging from third-party data centers to rental car companies, and a recent survey found that 45 percent of these companies have not only established programs to reduce their greenhouse gas emissions (GHG) but have also set specific targets to do so.[53] As a heavyweight in the corporate world, IBM is well positioned to make a difference through supply chain leadership.

IBM's supply chain program was established the same year that IBM achieved a remarkable environmental success. It took over five years and extensive coordination with many suppliers, but in 2010, IBM became the first computer manufacturer to eliminate the use of perfluorooctane sulfonate and perfluorooctanoic acid compounds from its chip manufacturing processes. The two compounds are known to be toxic to both humans and animals.[54]

IBM set aggressive goals for emissions reduction, and the company requires all its suppliers to establish management programs to implement environmentally responsible programs, and to measure and report their performance toward meeting environmental goals. Moreover, all of the company's "first-tier" suppliers must ensure that their own supplies meet or exceed these goals.[55] These programs must at the very least track carbon emissions and waste management.[56]

IBM is not the only IT giant to receive the EPA's Climate Leadership Award. Cisco Systems and SAP have both recently received the same award. Cisco uses its supply chain program to score its suppliers, and those scores impact which companies Cisco conducts business with. Cisco also conducts independent third-party audits of its suppliers to make sure they are accurately reporting on their progress.[57] SAP has created technology for its supply chain environmental programs, which the company claims reduces carbon emissions by 2.5 million tons annually—saving approximately $500 million in energy costs.[58]

Both IBM and Cisco are members of the Carbon Disclosure Project (CDP). Funded by numerous institutions and governments around the world, CDP works with thousands of companies to reduce GHG emissions, create sustainable water use programs, reduce deforestation, and—most notably—create programs that cascade the environmental commitments of large companies down the supply chain.[59]

Discussion Questions

1. Why does IBM's supply chain program have such a large impact on environmental health?
2. How do companies like Cisco ensure that their suppliers are complying with their supply chain programs?
3. How might IBM influence members of its supply chain to follow its environmental program?

2. E-Verify

U.S. law requires that companies operating in the United States only employ individuals who are legally permitted to work in the United States. To this end, all U.S. employers must complete and retain a Form I-9: Employment Eligibility Verification for each individual (both citizens and noncitizens) they hire in the United States. An employer must examine the employment eligibility and identity documents presented by a new employee to determine whether the documents reasonably appear to be genuine and relate to the individual; the employer must then record the document information on the Form I-9 for that employee. The list of acceptable documents includes documents that (1) establish both identity and employment authorization (U.S. passport, permanent resident card, etc.), (2) establish identity only (driver's license or photo ID card issued by a local, state, or federal government), or (3) establish authorization to work only (Social Security card, certificate of birth, etc.).[60]

E-Verify is an Internet-based system run by the U.S. Department of Homeland Security that allows employers to electronically verify the employment authorization of their newly hired employees.[61] The program compares information from an employee's Form I-9 to data in U.S. government records. If the data matches, the employee is eligible to work in the United States. If there is a mismatch, E-Verify alerts the employer, and the employee has eight work days to contact either the Social Security Administration or the Department of Homeland Security (depending on the source of the data mismatch) to start resolving the problem. During this eight-day period, and during the time it takes for the data mismatch to be further researched by the government agencies, the employee cannot be terminated.

In a 2011 ruling involving Arizona state law, the U.S. Supreme Court affirmed that states may constitutionally mandate the use of E-Verify for all employers within a given state. The states are greatly divided on this issue—some states have passed laws requiring all employers to use E-Verify to determine the eligibility of new hires; some just require public employers and government contractors to use E-Verify; and some require just private employers with more than a specified number of workers to use E-Verify. In some states, the decision to use E-Verify is being made at the county and city level.[62]

The number of employers who use E-Verify is increasing rapidly, almost doubling between 2010 (when 226,538 employers used the system) and 2012 (at which time 404,295 used it).[63] An immigration bill proposed by the U.S. Senate in 2013 would require all companies with 500 or more employees to adopt E-Verify within three years.[64]

According to a 2010 analysis of E-Verify conducted by an outside consulting firm on behalf of the U.S. Citizenship and Immigration Services, 4.1 percent of initial responses from the E-Verify system were inconsistent with the worker's actual employment eligibility status. Of those erroneous responses, 0.75 percent related to workers who were initially determined to be not authorized to work but who were in fact authorized, and 3.35 percent related to workers who were determined to be employment authorized but who were not actually eligible to do so.[65]

By 2012, however, the percent of mismatches was down to 1.35 percent. Only 0.09 percent of employees were confirmed as eligible for employment after an initial mismatch, while 1.26 percent were found to be in fact ineligible.[66]

One limit of E-Verify is that the system cannot detect all cases of identity fraud. In fact, the U.S. Immigration and Customs Enforcement (ICE) has conducted some of its largest raids of unauthorized workers at companies that use the E-Verify program. In 2011, for example, ICE raided Howard Industries' electrical transformer plant in Mississippi and found about 600 unauthorized workers, many of who had used identification data of someone other than themselves.[67]

The system's less than 100 percent accuracy rate and failure to identify unauthorized workers, including some workers committing identity fraud, has raised many political concerns and emotional responses. In order to reduce errors due to identity theft, the ICE recently implemented a photo tool that matches the photo submitted with the I-9 documents with photos in government records and with the actual employee. However, employers can choose to opt out of submitting a photograph of their employees.[68] Additional government databases may be integrated into the E-Verify matching process to improve accuracy.[69]

In addition to accuracy issues, there is concern that mandatory use of E-Verify will harm authorized workers and lead to discrimination. Opponents also fear it will create additional work for human resource departments in terms of updating personnel records, and initiating and following up on requests to various government agencies.

Meanwhile, proponents argue that the accuracy of the E-Verify system will improve over time and as further enhancements are made. They believe that it is fair to ask employers to do a quick check of each employee to ensure that they are hiring authorized workers. With the high level of unemployment, supporters of E-Verify believe that steps should be taken to ensure that jobs go to authorized workers.

Discussion Questions

1. Do you support the implementation of enhancements such as photo matching and access to additional government databases to improve the accuracy of the E-Verify system? Why or why not?
2. If you were the owner of a small business, would you use the E-Verify system to screen prospective workers? Why or why not?
3. Would you favor mandatory use of the E-Verify system at large corporations and government agencies? Why or why not?

3. Problems with Suppliers

Many computer hardware manufacturers rely on foreign companies to provide raw materials; build computer parts; and assemble hard drives, monitors, keyboards, and other components. While there are many advantages to dealing with foreign suppliers, hardware manufacturers may find certain aspects of their business (such as quality and cost control, shipping, and communication) more complicated when dealing with a supplier in another country.

In addition to these fairly common business problems, hardware manufacturers are sometimes faced with serious ethical issues relating to their foreign suppliers. Two such issues that have recently surfaced involve (1) suppliers who run their factories in a manner that is unsafe or

unfair to their workers and (2) raw materials suppliers who funnel money to groups engaged in armed conflict, including some that commit crimes and human rights abuses.

In February 2009, alarming information came to light about the Meitai Plastics and Electronics factory in Dongguan City, in China's Guangdong province. This factory, in fact, represents an extreme example of a supplier who runs its factory in an unsafe and unfair manner. Meitai Plastics employs 2,000 workers, mostly young women, who make computer equipment and peripherals—such as printer cases and keyboards—for Dell, IBM, Lenovo, Microsoft, and Hewlett-Packard products.[70] Based on research conducted between June 2008 and January 2009, the National Labor Committee (a human rights organization based in the United States) published a report in February 2009 highly critical of the work environment at the factory.[71]According to the report, young workers were required to sit on hard wooden stools for 12 hours a day, working on an assembly line that never stopped. Workers were prohibited from talking, listening to music, raising their heads from their work, or putting their hands in their pockets. Employees were fined for stepping on the grass of the factory grounds, not trimming their fingernails, and for being even one minute late. A worker who needed to use the restroom had to wait until there was a group break.

The average workweek consisted of 74 hours, with a take-home pay of $57.19—well below the amount necessary to meet subsistence-level needs in China. If a worker took a Sunday off, she was docked one-and-a-half-day's wages. Workers were housed 10 to 12 per dorm room. The dorms had no air conditioning, and temperatures in the rooms could reach the high 90s in the summer. Workers were required to walk down several floors to get hot water in a small bucket to use for personal hygiene.[72]

Manufacturers who use rare raw materials face another ethical issue related to the use of foreign suppliers: how to ensure that their suppliers do not funnel money to groups that engage in armed conflict or commit crimes and human rights abuses. Manufacturers of computers, digital cameras, cell phones, and other electronics frequently purchase rare minerals such as gold, tin, tantalum, and tungsten for use in their products. Unfortunately, some of these purchases are helping to finance the deadliest conflict in the world today—the war in the Democratic Republic of Congo. The war began in 1998 and has dragged on long after a peace agreement was signed in 2003. During the war and its aftermath, over 5 million people have died—mostly from disease and starvation—making it the deadliest conflict since World War II.[73]

In Congo, many mines are controlled by groups that engage in armed conflict and inflict human rights abuses on local populations. The Enough Project's "Raise Hope for Congo" campaign is trying to get large electronics firms to trace and audit their supply chains to ensure that their suppliers do not source minerals from mines in Congo that are controlled by armed groups. This is often easier said than done because of the long, complex supply chain and often disreputable middlemen involved in the minerals trade. As manufacturers struggle with these issues, some are trying to use their influence to demand that their suppliers stop sourcing from mines that continue to fund violence in Congo and elsewhere.[74]

Discussion Questions

1. What responsibility does an organization have to ensure that its suppliers and business partners behave ethically? To whom is this responsibility owed?
2. How can an organization monitor the business practices of its suppliers and business partners to determine if they are behaving in an ethical manner?

3. Is it good business practice to refuse to do business with a supplier who provides good quality materials at a low cost but who behaves in an unethical manner? How can senior management justify its decision to do business instead with a supplier who provides lower-quality or higher-priced materials but behaves in an ethical manner?

End Notes

[1] Daniel Fisher, "With Autonomy, H-P Bought an Old-Fashioned Accounting Scandal. Here's How It Worked," *Forbes*, November 20, 2012, www.forbes.com/sites/danielfisher/2012/11/20/with-autonomy-h-p-bought-an-old-fashioned-accounting-scandal.

[2] Julia Love, "In Wake of Autonomy Scandal, HP's Lawyers Wonder What's Next," *American Lawyer*, December 18, 2012, www.americanlawyer.com/PubArticleAL.jsp?id=1355662878654&slreturn=20130506105257.

[3] Jeffrey McCracken, Serena Saitto, and Aaron Ricadela, "Hewlett-Packard to Buy Autonomy for $10.3 Billion, Weighs PC Unit Spinoff," August 18, 2011, www.bloomberg.com/news/2011-08-18/hp-said-to-be-near-10-billion-autonomy-takeover-spinoff-of-pc-business.html.

[4] "HP and Autonomy: Conflicting Accounts," *The Economist*, November 20, 2012, www.economist.com/blogs/schumpeter/2012/11/hp-and-autonomy.

[5] Daniel Fisher, "With Autonomy, HP Bought an Old-Fashioned Accounting Scandal. Here's How It Worked," *Forbes*, November 20, 2012, www.forbes.com/sites/danielfisher/2012/11/20/with-autonomy-h-p-bought-an-old-fashioned-accounting-scandal.

[6] Ben Rooney, "Q&A with Autonomy Founder Mike Lynch on H-P Allegations," *Wall Street Journal*, November 20, 2012, http://blogs.wsj.com/digits/2012/11/20/qa-with-autonomy-founder-mike-lynch-on-h-p-allegations.

[7] Sean Patterson, "Autonomy Audit Firm Denies Knowledge of HP Fraud Claims," *WebPro News*, November 21, 2012, www.webpronews.com/autonomy-auditor-denies-knowledge-of-hps-fraud-claims-2012-11.

[8] Brid-Aine Parnell, "HP Knew Autonomy Was a Duff Buy, Claim HP Shareholders in $1bn Suit," *The Register*, May 8, 2013, www.theregister.co.uk/2013/05/08/hp_autonomy_shareholder_lawsuit.

[9] Katherine Rushton, "HP Boss Meg Whitman Admits Autonomy Row Hit Morale," *The Telegraph*, April 10, 2013, www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/electronics/9984271/HP-boss-Meg-Whitman-admits-Autonomy-row-hit-morale.html.

[10] Shane McGlaun, "HP Chairman Steps Down in the Wake of Autonomy Fiasco," *Daily Tech* (blog), April 5, 2013, www.dailytech.com/HP+Chairman+Steps+Down+in+the+Wake+of+Autonomy+Acquisition+Fiasco/article30292.htm.

[11] Brid-Aine Parnell, "HP Knew Autonomy Was a Duff Buy, Claim HP Shareholders in $1bn Suit," *The Register*, May 8, 2013, www.theregister.co.uk/2013/05/08/hp_autonomy_shareholder_lawsuit.

[12] Stuart Zweben, "2009-2010 Taulbee Survey: Undergraduate CS Degree Production Rises; Doctoral Production Steady," May 2011, www.cra.org/uploads/documents/resources/crndocs/issues/0511.pdf.

[13] C. Bret Lockard and Michael Wolf, "Employment Outlook: 2010-2020, Occupational Employment Projections to 2020," *Monthly Labor Review*, January 2012, www.bls.gov/opub/mlr/2012/01/art5full.pdf.

[14] Bill Virgin, "Microsoft Settles 'Permatemp' Suits," *Seattle-Post Intelligencer*, December 13, 2000.

[15] "What Is H-1B Visa?," Path2USA, www.path2usa.com/what-is-h1b-visa (accessed June 17, 2013).

[16] U.S. Citizenship and Immigration Services, U.S. Department of Homeland Security, "Characteristics of H-1B Specialty Occupation Workers," March 12, 2012, www.uscis.gov/USCIS/Resources/Reports%20and%20Studies/H-1B/h1b-fy-11-characteristics.pdf.

[17] U.S. Citizenship and Immigration Services, U.S. Department of Homeland Security, "Characteristics of H-1B Specialty Occupation Workers," March 12, 2012, www.uscis.gov/USCIS/Resources/Reports%20and%20Studies/H-1B/h1b-fy-11-characteristics.pdf.

[18] Patrick Thibodeau, "Hiring H-1B Visa Workers Trims U.S. Tech Workers' Wages, *PC World*, April 19, 2009, www.techhive.com/article/163383/h1b_visa_workers_trim_us_tech_worker_wages.html.

[19] Stuart Anderson, "No Hiring New H-1B Visa Holders for the Next 15 Months," *Forbes*, April 17, 2013, www.forbes.com/sites/stuartanderson/2012/06/13/no-hiring-new-h-1b-visa-holders-for-the next -15-months/.

[20] "H-1B Visa Application Process," www.h1base.com/visa/work/H1B%20Visa%20Application%20Regular%20Process/ref/1166/ (accessed June 16, 2013).

[21] Patrick Thibodeau, "Troubled H-1B Fraud Case Ends Quietly," *Computerworld*, May 16, 2011, www.computerworld.com/s/article/9216694/Troubled_H_1B_fraud_case_ends_quietly.

[22] Don Tennant, "U.S. Officials in Texas Arrest Six on Charges of H-1B Visa Fraud," *IT Business Edge*, March 5, 2013, www.itbusinessedge.com/blogs/from-under-the-rug/u.s.-officials-in-texas-arrest-six-on-charges-of-h-1b-visa-fraud.html.

[23] "Most Multinational Companies Use IT Outsourcing: Study," *IT World Canada*, February 25, 2010, www.itworldcanada.com/news/most-multinational-companies-use-it-outsourcing-study/140078.

[24] "Where Is Your Software From?" *TechByter Worldwide* (blog), January 11, 2009, www.techbyter.com/2009/20090111.html.

[25] 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.

[26] Diana ben-Aron, "Accenture Offers Buyouts to Finnish, U.K. Ex-Nokia Employees," *Bloomberg*, February 13, 2012, www.bloomberg.com/news/2012-02-13/accenture-offers-buyouts-to-finnish-u-k-ex-nokia-employees.html.

[27] David Ranii, "IT Staff Is Cut in Latest Dex Layoff," *News Observer*, June 3, 2011, www.newsobserver.com/2011/06/03/1244242/it-staff-is-cut-in-latest-dex.html.

[28] Craig Schneider, "Human Error to Blame for Grady Data Breach," *Atlanta Journal-Constitution*, September 23, 2008, http://downsizedagain.blogspot.com/2008_09_01_archive.html.

[29] Department of Justice, "Press Release: Justice Department Recovers Nearly $5 Billion in False Claims Act Cases in Fiscal Year 2012," December 4, 2012, www.justice.gov/opa/pr/2012/December/12-ag-1439.html.

[30] "False Claims Law," Fact Bites, www.factbites.com/topics/False-Claims-Law (accessed July 12, 2013).

[31] "Types of Qui Tam Cases," Whistleblower Info, www.whistleblowingprotection.org/?q=node/14 (accessed July 12, 2013).

[32] "False Claims Act/Qui Tam FAQ," National Whistleblowers Center, www.whistleblowers.org/index.php?Itemid=64&id=3 (accessed July 12, 2013).

[33] Phillips & Cohen LLP, "Press Release: Verizon Pays $93.5M to Settle Whistleblower Suit," *Bloomberg*, April 4, 2011, www.bloomberg.com/apps/news?pid=conewsstorytkr=VZ:US&sid=at4wiS2mjR74.

[34] Mike Scarcella, "Whistleblower in Verizon Case Demands Bigger Cut of $93.5M Settlement," *Corporate Counsel*, June 24, 2011, www.law.com/corporatecounsel/PubArticleCC.jsp?id=1202498286173&Whistleblower_in_Verizon_Case_Demands_Bigger_Cut_of_935M_Settlement&slreturn=20130612152446.

[35] Rik Myslewski, "Investor Sues Oracle Over $20m in Whistleblower Payout," *The Register*, March 23, 2012, www.theregister.co.uk/2012/03/23/oracle_sued_by_shareholder/print.html.

[36] "False Claims Act/Qui Tam FAQ," National Whistleblowers Center, www.whistleblowers.org/index.php?Itemid=64&id=3 (accessed July 12, 2013).

[37] Federal Accountability Initiative for Reform, "The Whistleblower's Ordeal," http://fairwhistleblower.ca/wbers/wb_ordeal.html (accessed June 18, 2013).

[38] 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.

[39] Steve Ragan, "TJX Fires Whistleblower—Was It Justified Action or Something Else?" *Tech Herald*, May 27, 2008, www.thetechherald.com/articles/TJX-fires-whistleblower-was-it-justified-action-or-something-else-(Update)/242.

[40] Brad Wells, "What Truly Makes a Computer 'Green'?," *OnEarth* (blog), September 8, 2008, www.onearth.org/node/658.

[41] 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#.UeCSz83D_IU.

[42] EPEAT, "New Branding for EPEAT Green Electronics Rating System," June 23, 2011, www.epeat.net/2011/06/news/new-branding-for-epeat-green-electronics-rating-system.

[43] Ricoh, "Electronic Product Environmental Assessment Tool: Recognizing Environmental Performance," www.ricoh-usa.com/about/epeat (accessed June 20, 2013).

[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] "Facts and Figures on E-Waste and Recycling," Electronics TakeBack Coalition, June 25, 2013, www.electronicstakeback.com/wp-content/uploads/Facts_and_Figures_on_EWaste_and_Recycling.pdf.

[46] "State Legislature: States Are Passing E-Waste Legislation," Electronics TakeBack Coalition, www.electronicstakeback.com/promote-good-laws/state-legislation (accessed July 12, 2013).

[47] Dell, "Dell's Worldwide Technology Recycling Options," www.dell.com/learn/us/en/uscorp1/corp-comm/globalrecycling (accessed July 12, 2013).

[48] Electronic Industry Citizenship Coalition, "Membership," www.eicc.info/MEMBERSHIP.htm (accessed June 27, 2013).

[49] Electronic Industry Citizenship Coalition Code of Conduct version 4.0 (2012), www-03.ibm.com/procurement/proweb.nsf/objectdocswebview/fileelectronic+industry+supply+code+of+conduct/$file/eicccodeofconductenglish.pdf.

[50] Electronic Industry Citizenship Coalition, "Membership," www.eicc.info/MEMBERSHIP.htm (accessed June 27, 2013).

[51] IBM, "Press Release: EPA Recognizes IBM for Climate Change Leadership," March 1, 2013, www-03.ibm.com/press/us/en/pressrelease/40518.wss.

[52] GreenBiz Staff, "IBM Racks Up Nearly $27 M in Energy Savings," *GreenBiz*, June 30, 2010, www.greenbiz.com/news/2010/06/30/ibm-racks-up-nearly-27m-energy-savings.

[53] IBM, "CDP Supply Chain Project," www.ibm.com/ibm/environment/supply/cdpscp.shtml (accessed June 14, 2013).

[54] Greener Computing Staff, "IBM Achieves First Full Phase-Out of Toxic Compounds," *Greener Computing*, March 2, 2010, www.greenbiz.com/news/2010/03/02/ibm-achieves-industry-first-phase-out-toxic-compounds.

[55] "EPA Recognizes IBM for Climate Change Leadership," IBM News Room, March 1, 2013, www-03.ibm.com/press/us/en/pressrelease/40518.wss.

[56] U.S. Environmental Protection Agency, "2013 Climate Leadership Award Winners," www.epa.gov/climateleadership/awards/2013winners.html (accessed June 14, 2013).

[57] U.S. Environmental Protection Agency, "2013 Climate Leadership Award Winners," www.epa.gov/climateleadership/awards/2013winners.html (accessed June 14, 2013).

[58] U.S. Environmental Protection Agency, "2012 Climate Leadership Award Winners," www.epa.gov/climateleadership/awards/2012winners.html (accessed June 14, 2013).

[59] Carbon Disclosure Project, "Catalyzing Business and Government Action," www.cdproject.net/en-US/Pages/About-Us.aspx (accessed June 14, 2013).

[60] Form I-9, Employment Eligibility Verification, Department of Homeland Security, U.S. Citizenship and Immigration Services, www.uscis.gov/files/form/i-9.pdf (accessed June 15, 2011).

[61] U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, "E-Verify: Questions and Answers," www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=51e6fb41c8596210VgnVCM100000b92ca60aRCRD&vgnextchannel=51e6fb41c8596210VgnVCM100000b92ca60aRCRD (accessed August 6, 2013).

[62] U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, "E-Verify: Questions and Answers," www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=51e6fb41c8596210VgnVCM100000b92ca60aRCRD&vgnextchannel=51e6fb41c8596210VgnVCM100000b92ca60aRCRD (accessed June 16, 2013).

[63] U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, "History and Milestones," www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=84979589cdb76210VgnVCM100000b92ca60aRCRD&vgnextchannel=84979589cdb76210VgnVCM100000b92ca60aRCRD (accessed June 16, 2013).

[64] Rosalind S. Helderman, "Inside the Immigration Bill: E-Verify Expansion Draws Fire," *Washington Post*, April 16, 2013, www.washingtonpost.com/blogs/post-politics/wp/2013/04/16/inside-the-immigration-bill-e-verify-expansion-draws-fire-from-civil-libertarians/.

[65] Representative Lamar Smith, "E-Verify Will Help American Jobs Go to Legal Workers," *The Hill's Congress Blog, The Hill*, June 21, 2011, http://thehill.com/blogs/congress-blog/politics/167509-e-verify-will-help-american-jobs-go-to-legal-workers.

[66] U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, "Statistics and Reports," www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextchannel=7c579589cdb76210VgnVCM100000b92ca60aRCRD (accessed June 16, 2013).

[67] Marc Rosenblum and Lang Hoyt, "Migration Fundamentals: The Basics of E-Verify, the US Employer Verification System," Migration Policy Institute, July 2011, www.migrationinformation.org/feature/display.cfm?ID=846.

[68] U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, "Photo Matching," www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=bbcbfb41c8596210VgnVCM100000b92ca60aRCRD&vgnextchannel=bbcbfb41c8596210VgnVCM100000b92ca60aRCRD (accessed June 15, 2013)

[69] Capital Immigration Law Group "Reports Highlights E-Verify Accuracy Problems," February 25, 2010, www.cilawgroup.com/news/2010/02/25/report-highlights-e-verify-accuracy-problems.

[70] Jason Gooljar, "Chinese Factory That Supplies IBM, Microsoft, Dell, Lenovo and Hewlett-Packard to Be Investigated," *Dissent Is Patriotic* (blog), February 15, 2009, www.jasongooljar.com/?tag=meitai-plastic-and-electronics.

[71] Tom Espiner, "Tech Coalition Launches Sweatshop Probe," *CNET*, February 14, 2009, http://news.cnet.com/8301-1001_3-10164325-92.html.

[72] National Labor Committee, "High Tech Misery in China: The Dehumanization of Young Workers Producing Our Computer Keyboards," February 2009, www.nlcnet.org/article.php?id=613.

[73] Joe Bavier, "Congo War-Driven Crisis Kills 45,000 A Month—Study," *Reuters*, January 22, 2008, www.reuters.com/article/2008/01/22/idUSL22802012._CH_.2400.

[74] The Enough Project, "Electronics Companies Respond to the Enough Project," www.raisehopeforcongo.org/responses (accessed July 4, 2011).

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—8th-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 your 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 (8th 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 20th-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 20th-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 common-sense 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 18th-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 20th 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 vs. 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 to borrow 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 (for example, 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 20th 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 20th 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 20th-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.

APPENDIX **B**

ANSWERS TO SELF-ASSESSMENT QUESTIONS

Chapter 1 answers: 1. morality; 2. Ethics; 3. Virtues; 4. code of principles; 5. Morals; 6. Corporate social responsibility; 7.Supply chain sustainability; 8. reputation; 9. vision and leadership; 10. Law; 11. Section 406 of the Sarbanes-Oxley Act; 12. renew investor's trust in the content and preparation of disclosure documents by public companies; 13. Code of ethics; 14. social audit; 15. formal ethics training; 16. problem definition; 17. Common good approach; 18. Problem definition

Chapter 2 answers: 1. d.; 2. IT; 3. stop the unauthorized copying of software produced by its members; 4. True; 5. Fraud; 6. Compliance; 7. d.; 8. Internal audit; 9. b.; 10. True; 11. Negligence; 12. code of ethics

Chapter 3 answers: 1. b.; 2. True; 3. exploit; 4. Virtualization; 5. False; 6. Zero-day attack; 7. CAPTCHA; 8. ransomware; 9. Distributed denial-of-service; 10. Trojan horse; 11. botnet; 12. Trustworthy computing; 13. risk assessment; 14. b; 15. False; 16. False

Chapter 4 answers: 1. c.; 2. discovery; 3. False; 4. b.; 5. True; 6. HIPAA; 7. d.; 8. Family Educational Rights and Privacy Act; 9. Katz; 10. Foreign Intelligence Surveillance Act; 11. a.; 12. True; 13. USA PATRIOT Act; 14. True; 15. Fair Information Practices; 16. True; 17. Cookie; 18. FTC

Chapter 5 answers: 1. First Amendment; 2. *Miller v. California*; 3. True; 4. True; 5. Section 230; 6. c.; 7. Internet censorship; 8. False; 9. Doxing; 10. False; 11. John Doe; 12. c.; 13. True; 14. True; 15. False; 16. CAN-SPAM

Chapter 6 answers: 1. d.; 2. patent; 3. True; 4. a.; 5. False; 6. Digital Millennium Copyright Act; 7. trademark; 8. cross-licensing; 9. fair use; 10. cc; 11. Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement; 12. False; 13. reverse engineering; 14. prior art; 15. True; 16. cybersquatting

Chapter 7 answers: 1. b.; 2. quality; 3. d.; 4. b.; 5. product liability; 6. software development methodology; 7. False; 8. defect; 9. quality assurance.; 10. b.; 11. a; 12. True; 13. b.; 14. failure mode and effect analysis (FMEA); 15. False; 16. negligence

Chapter 8 answers: 1. b.; 2. productivity; 3. a.; 4. d.; 5. Digital divide; 6. c.; 7. a.; 8. True; 9. E-rate; 10. b.; 11. True; 12. electronic health record (EHR); 13. meaningful use

Chapter 9 answers: 1. social shopping network Web site; 2. c.; 3. Linked-In; 4. True; 5. b.; 6. False; 7. MySpace; 8. False; 9. False; 10. d.; 11. False; 12. brand awareness

Chapter 10 answers: 1. d.; 2. a; 3. d.; 4. True; 5. H-1B; 6. d. 7. True; 8. b.; 9. False; 10. c.; 11. d.; 12. True; 13. Wipro; 14. gold

GLOSSARY

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) 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 of 2009 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.

anonymous expression The expression of opinions by people who do not reveal their identities.

anonymous remailer A company that provides a service in which an originating IP number (computer address) is stripped from an email message before the message is sent on to its destination.

anti-SLAPP laws Laws designed to reduce frivolous lawsuits filed against citizens and community groups who oppose corporations, government officials, and others.

antivirus software Software that regularly scans a computer's memory and disk drives for viruses.

audit committee A subgroup of the board of directors that provides assistance to the board 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 function.

avatar A virtual world visitor's representation of him- or herself—usually in the form of a human but sometimes in some other form, such as an animal or mythical creature.

Bathsheba syndrome The moral corruption of people in power often facilitated by a tendency for people to look the other way when their leaders act inappropriately.

beacon A small piece of software that runs on a Web page and is able to track what a viewer is doing on the page, such as what is being typed or where the mouse is moving.

black-box testing A form 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). If the unit demonstrates the expected behaviors for all the input data in the test suite, it passes the test.

body of knowledge An agreed-upon set of skills and abilities that all licensed professionals in a particular type of profession must possess.

botnet A large group of computers 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 The failure of a product to meet the terms of its warranty.

bribery The act of providing money, property, or favors to someone in business or government to obtain a business advantage.

bring your own device (BYOD) A business policy that permits and encourages employees to use their own mobile devices

(smartphones, tablets, or laptops) to access company computing resources and applications.

business information system A set of interrelated components—including hardware, software, databases, networks, people, and procedures—that collects data, processes it, and disseminates the output.

Business Software Alliance (BSA) A trade group that represents the world's largest software and hardware manufacturers; its mission is to stop the unauthorized copying of software produced by its members.

Capability Maturity Model Integration (CMMI) A process improvement approach developed by the Software Engineering Institute at Carnegie Mellon that defines the essential elements of effective processes.

CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) Software that generates and grades tests that humans can pass but all but the most sophisticated computer programs cannot.

certification A recognition that a professional possesses a particular set of skills, knowledge, or abilities—in the opinion of the certifying organization.

chief privacy officer (CPO) A senior manager within an organization whose role is to both ensure that the organization does not violate government regulations and reassure customers that their privacy will be protected.

Child Online Protection Act (COPA) A law that states "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." This law was eventually found to be unconstitutional.

Children's Internet Protection Act (CIPA) An act that requires 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) A 1998 law that requires Web sites 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 13 years of age.

click-stream data Information gathered by monitoring a consumer's online activity through the use of electronic cookies.

cloud computing An environment in which software and data storage are services provided via the Internet (the cloud); the services are run on another organization's computer hardware and are accessed by a Web browser.

CMMI *See* Capability Maturity Model Integration (CMMI).

CMMI-Development (CMMI-DEV) An application of CMMI that is 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 An employment situation in which two employers have actual or potential legal rights and duties with respect to the same employee or group of employees.

collusion Cooperation between two or more people, often an employee and a company outsider, to commit fraud.

commoditization The transformation of goods or services into commodities that offer nothing to differentiate themselves from those offered by competitors. Commoditized goods and services are sold strictly on the basis of price.

common good approach An approach to ethical decision making based on a vision of

society as a community whose members work together to achieve a common set of values and goals.

Communications Act of 1934 The law that established the Federal Communications Commission and gave it responsibility for regulating all non-federal-government use of radio and television broadcasting and all interstate telecommunications—including wire, satellite, and cable—as well as all international communications that originate or terminate in the United States.

Communications Assistance for Law Enforcement Act (CALEA) A 1994 law that amended both the Wiretap Act and EGPA; it requires 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) A part of the 1996 Telecommunications Act directed at protecting children from online pornography; it was eventually ruled unconstitutional.

competitive intelligence Legally obtained information gathered using sources available to the public; used to help a company gain an advantage over its rivals.

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 it is admissible as evidence in a court of law.

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 A defense in a negligence case in which the defendant argues that the plantiff's own actions contributed to his or her injuries.

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act A 2004 law that specifies requirements that commercial emailers must follow when sending out messages that advertise or promote a commercial product or service.

cookie An electronic text file that a Web site downloads to visitors' hard drives so it can identify them 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 The concept that an organization should act ethically by taking responsibility for the impact of its actions on the environment, the community, and the welfare of its employees.

cracker Someone who breaks into other people's networks and systems to cause harm.

cyberbullying The harassment, torment, humiliation, or threatening of one minor by another minor or group of minors via the Internet or cell phone.

cybercriminal An individual, motivated by the potential for monetary gain, who hacks into computers to steal, often by transferring money from one account to another to another.

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.

cyberterrorist An individual who launches computer-based attacks against other computers or networks in an attempt to intimidate or coerce a government in order to advance certain political or social objectives.

data breach The unintended release of sensitive data or the access of sensitive data by unauthorized individuals.

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 harms another person.

deliverables The products of a software development process, such as statements of requirements, flowcharts, and user documentation.

digital divide The gulf between those who do and those who do not have access to modern information and communications technology, such as cell phones, personal computers, and the Internet.

Digital Millennium Copyright Act (DMCA) An act that implements two WIPO treaties in the United States. It also makes it illegal to circumvent a technical protection or develop and provide tools that allow others to access a technologically protected work. It also limits the liability of online service providers for copyright infringement by their subscribers or customers.

distributed denial-of-service attack (DDoS) 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 Involves the examination of Interent records in an attempt to reveal the identity of an anonymous poster.

due diligence The investigation of all areas of an organization prior to agreeing to a merger or other important transaction.

duty of care The obligation to protect people against any unreasonable harm or risk.

dynamic testing An approach to software QA testing in which the code for a completed unit of software is tested by entering test data and comparing the actual results with the expected results.

Education Rate (E-Rate) program A program created through the Telecommunications Act of 1996; its primary goal is to help schools and libraries obtain access to state-of-the-art services and technologies at discounted rates.

Electronic Communications Privacy Act of 1986 (ECPA) A law focusing on 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 to record 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 legal actions and proceedings.

electronic health record (EHR) A computer-readable record of health-related information on an individual; can include patient demographics, medical history, family history, immunization records, laboratory data, health problems, progress notes, medications, vital signs, and radiology reports. Data can be added to an EHR based on each patient encounter in any healthcare delivery setting.

Electronic Industry Citizenship Coalition (EICC) An industry organization established to promote a common code of conduct for the electronics and information and communications technology (ICT) industry.

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.

email spam The abuse of email systems to send unsolicited email to large numbers of people.

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.

ethics A set of beliefs about right and wrong behavior within a society.

European Data Protection Regulation Proposed regulation to enforce a single set of rules for data protection across the EU.

European Union Data Protection Directive A directive passed by the European Union in 1998 that requires any company doing business within the borders of 15 western European nations to implement a set of privacy directives on the fair and appropriate use of information; it also bars the export of data to countries that do not have comparable data privacy protection standards.

exploit An attack on an information system that takes advantage of a particular system vulnerability.

failure mode and effects analysis (FMEA) A 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 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 A law passed in 1970 that regulates the operations of credit-reporting bureaus, including how they collect, store, and use credit information.

Fair Information Practices A set of eight principles created by the Organisation for Economic Co-operation and Development that provides guidelines for the ethical treatment of consumer 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.

fairness approach An approach to ethical decision making that focuses on how fairly actions and policies distribute benefits and burdens among people affected by the decision.

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. These rights transfer to the student once the student attains the age of 18 or attends a school beyond the high school level.

firewall A hardware or software device that serves as a barrier 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.

Foreign Corrupt Practices Act (FCPA) A federal law 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, agents of foreign governments, or foreign organizations.

Foreign Intelligence Surveillance Act (FISA) An act passed in 1978 that describes procedures for the electronic surveillance and collection of foreign intelligence information in communications between foreign powers and agents of foreign powers.

Foreign Intelligence Surveillance Act Amendments Act An act that granted NSA expanded authority to collect, without court-approved warrants, international communications as they flow through U.S. telecom network equipment and facilities.

fraud The crime of obtaining goods, services, or property through deception or trickery.

Freedom of Information Act (FOIA) A law passed in 1966 and amended in 1974 that grants citizens the right to access certain information and records of the federal government upon request.

globalization The process of interaction and integration among the people, companies, and governments of different nations.

government license A government-issued permission to engage in an activity or to operate a business; it is generally administered at the state level and often requires that the recipient pass a test of some kind.

Gramm-Leach-Bliley Act (GLBA) A 1999 bank deregulation law, also known as the Financial Services Modernization Act, which granted banks the right to offer investment, commercial banking, and insurance services through a single entity.

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.

hacker Someone who tests the limitations of information systems out of intellectual curiosity—to see if he or she can gain access.

hacktivism Hacking to achieve a political or social goal.

Health Information Technology for Economic and Clinical Health Act (HITECH Act) Part of the $787 billion 2009 American Recovery and Reinvestment Act economic stimulus plan. HITECH is intended to increase the use of health information technology by: (1) requiring the government to develop standards for the nationwide electronic exchange and use of health information; (2) providing $20 billion in incentives to encourage doctors and hospitals to use EHRs to electronically exchange patient healthcare data; (3) saving the government $10 billion through improvements in the quality of care and care coordination and through reductions in medical errors and duplicate care; and (4) strengthening the protection of identifiable health information.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) A law 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.

identity theft The act of stealing key pieces of personal information to impersonate a person.

industrial espionage The use of illegal means to obtain business information not available to the general public.

industrial spy Someone who uses illegal means to obtain trade secrets from competitors.

information privacy 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).

integration testing A form of software testing in which individual 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.

intentional misrepresentation Fraud that occurs when a seller or lessor either misrepresents the quality of a product or conceals a defect in it.

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 Web sites 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 identifies possible intrusions from outside the organization or misuse from within the organization.

IT user A person for whom a hardware or software product is designed.

Jacob Watterling Crimes Against Children and Sexually Violent Registration Act An act that set the initial requirements for sex offender registration and notificiation in the United States.

John Doe lawsuit A lawsuit in which the identity of the defendant is temporarily unknown, typically because the defendant is communicating anonymously or using a pseudonym.

lamer A technically inept hacker. *See also* script kiddie.

law A system of rules that tells us what we can and cannot do. Laws are enforced by a set of institutions.

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.

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 that executes when it is triggered by a specific event.

massive multiplayer online role playing games (MMORPG) A multiplayer online game that provides a huge online world in which players take on the role of a character and control that character's action; players can interact with one another to compete in online games and challenges that unfold according to the online world's rules and storyline.

material breach of contract The failure of one party to perform certain express or implied obligations, which impairs or destroys the essence of the contract.

Miller v. California The 1973 Supreme Court case that established a test to determine if material is obscene and therefore not protected by the First Amendment.

misrepresentation The misstatement or incomplete statement of a material fact.

modularization The act of breaking down a production or business process into smaller components.

moral code A set of rules that establishes the boundaries of generally accepted behavior within a society.

morality Social conventions about right and wrong that are widely shared throughout a society.

morals One's personal beliefs about right and wrong.

negligence The failure to do what a reasonable person would do, or doing something that a reasonable person would not do.

negligent insider A poorly trained and inadequately managed employee who means well but who has the potential to cause much damage.

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 clause Terms of an employment contract that prohibit an employee from revealing secrets.

N-version programming A form of redundancy in which two or more (n) computer systems execute a series of program instructions simultaneously.

offshore outsourcing A form of outsourcing in which the services are provided by an organization whose employees are in a foreign country. *See also* outsourcing.

One Laptop per Child (OLPC) A nonprofit organization whose goal is to provide children around the world with low-cost laptop computers to aid in their education.

online virtual world A shared multimedia computer-generated environment in which users, represented by avatars, can act, communicate, create, retain ownership of what they create, and exchange assets, including currency, with each other.

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 agree (either implicitly or by default) to allow an organization to collect and share one's personal data with other institutions.

opt out To refuse to give an organization the right to collect and share one's personal data with unaffiliated parties.

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.

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 farming An unethical strategy of influencing a standards organization to make use of a patented item without revealing the existence of a patent; later, the patent holder might demand royalties from all implementers of the standard.

patent infringement A violation of the rights secured by the owner of a patent; occurs when someone makes unauthorized use of another's patent.

patent troll A firm that acquires patents for the purpose of licensing the patents to others rather than manufacturing anything itself.

pen register A device that records electronic impulses to identify the numbers dialed for outgoing calls.

personalization software Software used by online marketers to optimize the number, frequency, and mixture of their ad placements as well as to evaluate how visitors react to new ads.

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.

prior art The existing body of knowledge that is available to a person of ordinary skill in the art.

Privacy Act of 1974 A law decreeing that no agency of the U.S. government can conceal 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.

problem statement A clear, concise description of the issue that needs to be addressed in a decision-making process.

product liability The liability of manufacturers, sellers, lessors, and others for injuries caused by defective products.

productivity The amount of output produced per unit of input.

profession A calling that requires specialized knowledge and often long and intensive academic preparation.

professional code of ethics A statement of the principles and core values that are essential to the work of a particular occupational group.

professional malpractice Breach of the duty of care by a professional.

project safety engineer An individual on a safety-critical system project who has explicit responsibility for the system's safety.

quality assurance (QA) Methods within the software development cycle designed to guarantee reliable operation of a product.

quality management Business practices that focus on defining, measuring, and refining the quality of the development process and the products developed during its various stages.

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 disables a computer or smartphone until the victim pays a fee or ransom.

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 use of multiple interchangeable components designed to perform a single function—in order to cope with failures and errors.

reliability The probability of a component or system performing without failure over its product life.

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 to Financial Privacy Act of 1978 An act that protects the financial records of financial institution customers from unauthorized scrutiny by the federal government.

risk The probability of an undesirable event occurring times the magnitude of the event's consequences if it does happen.

risk assessment The process of assessing security-related risks from both internal and external threats to an organization's computers and networks.

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 injury or death.

Sarbanes-Oxley Act A bill whose goal was to renew investors' trust in corporate executives and their firms' financial reports; the act led to significant reforms in the content and preparation of disclosure documents by public companies.

script kiddie A technically inept hacker. *See also* lamer.

security audit A process that evaluates whether an organization has a well-considered security policy in place and if it is being followed.

security policy A written statement that defines an organization's security

requirements, as well as the controls and sanctions needed to meet those requirements.

Sex Offender Registration and Notification (SORNA) Provisions Part of the Adam Walsh Child Protection and Safety Act that set national standards for which sex offenders must register and what data must be captured.

sexting Sending sexual messages, nude or seminude photos, or sexually explicit videos over a cell phone.

slander An oral defamatory statement.

strategic lawsuit against public participation (SLAPP) A lawsuit brought by corporations, government officials, and others against citizens and community groups who oppose them on matters of public interest.

smart card A form of debit or credit card that contains a memory chip that is updated with encrypted data every time the card is used.

smishing A variation of phishing in which victims receive a legitimate-looking SMS text message on their phone telling them to call a specific phone number or to log on to a Web site.

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 network advertising Advertising using social networks to communicate and promote the benefits of products and services.

social networking Web site A Web site that creates an online community of Internet users that enables members to break down time, distance, and cultural barriers and interact with others by sharing opinions, insights, information, interests, and experiences.

social shopping Web site A Web site that brings shoppers and sellers together in a social networking environment in which members can share information and make recommendations while shopping online.

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 piracy The act of illegally 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.

spear-phishing A variation of phishing in which the phisher sends fraudulent emails to a certain organization's employees. The phony emails are designed to look like they came from high-level executives within the organization.

spyware Keystroke-logging software downloaded to users' computers without their knowledge or consent.

stakeholder Someone who stands to gain or lose depending on how a situation is resolved.

stalking app Cell phone spy software that can be loaded onto someone's phone to perform location tracking, record calls, view every text message or picture sent or received, and record the URL of any Web site visited.

standard A definition that has been approved by a recognized standards organization or accepted as a de facto standard by a particular industry.

static testing The use of special software programs called static analyzers to look for suspicious patterns in programs that might indicate a defect.

store-and-forward telemedicine A form of telemedicine in which data, sound, images, and video are acquired from a patient and then transmitted to a medical specialist for later evaluation.

strict liability A type of product liability in which a defendant is held responsible for injuring another person, regardless of negligence or intent.

submarine patent A patented process or invention that is hidden within a standard and which is not made public until after the standard is broadly adopted.

sunset provision A provision that terminates or repeals a law or portions of it after a specific date, unless further legislative action is taken to extend the law.

system testing A form of software testing in which 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 The component of telehealth that provides medical care to people at a location different from healthcare providers.

telework A work arrangement in which an employee works away from the office—at home, at a client's office, in a hotel—literally anywhere; also known as telecommuting.

Title III of the Omnibus Crime Control and Safe Streets Act A component of a 1968 law (amended in 1986) that regulates the interception of wire 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. It represents something of economic value that has required effort or cost to develop and that has some degree of uniqueness or novelty.

trademark A logo, package design, phrase, sound, or word that enables a consumer to differentiate one company's products from another's.

transparency Any attempt to reveal and clarify any information or processes that were previously hidden or unclear.

trap and trace A device that records electronic impulses to identify the originating number for incoming calls.

Trojan horse A program in which malicious code is hidden inside a seemingly harmless program.

trustworthy computing A method of computing that delivers secure, private, and reliable computing experiences based on sound business practices.

USA PATRIOT Act A law passed in 2001 that gave sweeping new powers to domestic law enforcement and to intelligence agencies, including increasing the ability of law enforcement agencies to search telephone, email, medical, financial, and other records, and easing restrictions on foreign intelligence gathering in the United States.

user acceptance testing Independent testing performed by trained end users to ensure that a system operates as expected.

utilitarian approach An approach to ethical decision making that states that you should choose the action or policy that has the best overall consequences for all people who are directly or indirectly affected.

vice A moral habit that inclines people to do what is generally unacceptable to society.

vehicle event data recorder 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.

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.

virtual machine A server with virtualization software is able to create several virtual machines each with their own operating system that run on that single server.

virtual private network (VPN) A technology that uses the Internet to relay communications, maintaining privacy through security procedures and tunneling protocols, which encrypt data at the sending end and decrypt it at the receiving end.

virtualization software A software program that emulates computer hardware by

enabling multiple operating systems to run on one computer host.

virtue A moral habit that inclines people to do what is generally acceptable to society.

virtue ethics approach An approach to ethical decision making that focuses on how you should behave and think about relationships if you are concerned with your daily life in a community.

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 A variation of phishing in which victims receive a voice mail telling them to call a specific phone number or log on to access a specific Web site.

warranty An assurance to buyers or lessees that a product meets certain standards of quality.

whistle-blowing An effort to attract public attention to a negligent, illegal, unethical, abusive, or dangerous act by a company or some other organization.

white-box testing A form of dynamic testing that treats the software unit as a device that has expected input and output behaviors and whose internal workings are known. White-box testing involves testing all possible logic paths through the software unit, with thorough knowledge of its logic.

worm A harmful program that resides in the active memory of a computer and duplicates itself.

zero-day attack An attack that takes place before the security community or software developer knows about the vulnerability or has been able to repair it.

zombie A computer that is part of a botnet and that is controlled by a hacker without the knowledge or consent of its owner.

INDEX

A

ABC News, Inc., 183
ACAD/Medre.A virus, 97
Accenture, 381–382
ACLU. *See* American Civil Liberties Union (ACLU)
ACM. *See* Association for Computing Machinery (ACM)
ACM Tech News, 55
ACPA. *See* Anticybersquatting Consumer Protection Act (ACPA)
action plan
  legal, 11
  for whistle-blowing, 390
activity logs, 111
Adam Walsh Child Protection and Safety Act, 349–350
Adelphia, 15
Adobe Systems, 46, 83, 234
Advanced Encryption Standard (AES), 132
advanced surveillance technology, 157–159
  anonymity and, 157–159
  camera surveillance, 157–158
  Fourth Amendment and, 157
  stalking app, 159
  vehicle event data recorders, 158–159
advertising
  company-owned social networking Web Site and, 342
  definition of, 339
  direct, 340
  group, 341–342
  indirect, through groups, 341–342
  social networking, 339–342
  using individual network of friends, 340–341
  viral marketing and, 342
Aegis radar, 279
AES. *See* Advanced Encryption Standard (AES)
Aetna, 381
Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), 224–225
AICPA. *See* American Institute of Certified Public Accountants (AICPA)
AIG. *See* American International Group (AIG)
Airbus 300, 279
AITP. *See* Association of Information Technology Professionals (AITP)
Alexander, Keith, 133
Alexander Automotive Group, 46
Ally Financial, 243
alternative decision making. *See also* decision making
  common good approach to, 24
  evaluation of, 22–24
  fairness approach to, 23
  identification of, 21–22
  selection of, 22–24
  utilitarian approach to, 23
  virtue ethics approach to, 23
Alwil Avast Internet Security 2012, 108
Amazon, 152–153, 336
Amenity Home, 345
America Invents Act, 230
American Bar Association, 60
American Civil Liberties Union (ACLU), 132–133, 184, 185, 188, 343
American Express, 341, 381
American Institute of Certified Public Accountants (AICPA), 385
American International Group (AIG), 5
American Recovery and Reinvestment Act, 139
American Superconductor (AMSC), 217–220
AMSC. *See* American Superconductor (AMSC)
Android
  exploits aimed at, 88
  Internet filtering on, 186
  Market Web Site, 61
  software piracy on, 61
  Tetris on, 223
anonymity
  advanced surveillance technology for, 157–159
  consumer profiling and, 154–155
  data breaches and, 151–153
  electronic discovery and, 153–154
  on Internet, 190–193
  John Doe lawsuits and, 192–193
  privacy and, 151–159
  Web, 191
  workplace monitoring and, 155–157
Anonymous, 191
anonymous expression, 190
anonymous remailer service, 191–192

anonymous speech, 193
Anticybersquatting Consumer Protection Act (ACPA), 243
anti-SLAPP laws, 190
antivirus software, 107–108
AOL, Inc., 191, 197
Apple
  App Store, 336
  bribery at, 50
  Business Software Alliance membership of, 46
  code of conduct of, 392
  green computing and, 391
  Greenpeace ratings of, 392
  iPad®, 7, 50, 342, 391
  iPhone®, 7, 49, 50, 88, 186, 223, 233, 238, 242, 302
  iPod®, 50, 223
  iTouch®, 223
  iTunes, 223
  Macintosh user interface of, 236
  noncompete agreements with, 234
  nondisclosure clauses for, 233
  open source code used by, 238
  patent infringement by, 153, 231
  Safari, 12, 154
Aramco (Saudi Arabian Oil Company), 96
Artist Arena, 140
Ashcroft v. American Civil Liberties Union, 185, 195
ASIS International, 102
Ask.fm, 346
Association for Computing Machinery (ACM), 55–56
Association of Corporate Counsel, 11
Association of Information Technology Professionals (AITP), 56, 60
A.T. Kearney, 382
ATM. *See* automated teller machine (ATM) card
AT&T, 131
audit committees, 65–66
Authors Guild, 223
AutoCAD software, 97
automated system rules, 104
automated teller machine (ATM) card, 94
Autonomy Corporation, 369–371
avatar, 351–352

B

Bank of America, 5, 91, 136, 304
Bank Secrecy Act, 6
Barclays, 370–371
Barr, William P., 228
Bathsheba syndrome, 6
BATS. *See* Better Alternative Trading System (BATS)
Beatles, 222
Beef Products, Inc., 183
behavior-based intrusion detection system, 106
Best Buy, 304
BET, 227
Better Alternative Trading System (BATS), 262, 263
Better Business Bureau, 180
Bieber, Justin, 140
Big Thunder Mountain Railroad roller coaster, 276
Bill of Rights, 134, 182, 191
Bing search engine, 236
BlackBerry®, 88, 238, 302
black-box testing, 272
Blase, Dan, 275
Blaster worm, 109
Blendtec, 342
Bloomberg, Michael, 158
Blumenthal, Richard, 349
board of directors, 14–15
body of knowledge, 59
Boeing, 132
Bondy, Joel, 42
B-1 visas, 47
botnet, 91–92
Brazilian Industrial Property Institute, 242
breach
  of contract, 49
  of data, 98, 151–153
  of duty of care, 60–61
  of warranty, 269
bribery, 50–52
bring your own device (BYOD) policies, 87
Brown & Williamson, 388
BSA. *See* Business Software Alliance (BSA)
BSkyB, 15
bullying, 191
Bush, George W., 133, 146
business ethics, 5–19
  corporate ethics and, 12–18
  corporate social responsibility and, 8–12
  ethical work environment and, 18–19
  good, importance of, 8–12
  of IBM, 6
business information system, 267
business practices, 10–11
Business Software Alliance (BSA), 46, 85
BYOD. *See* bring your own device (BYOD) policies

C

Cablegate incident, 7
CALEA. *See* Communications Assistance for Law Enforcement Act (CALEA)
California Department of Public Health, 152
California Division of Occupational Safety and Health, 276
California Online Privacy Protection Act, 65
camera surveillance, 157–158
CAN-SPAM. *See* Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act
Capability Maturity Model Integration (CMMI), 273–275
Capital Area Transportation Authority (CATA), 344
CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) software, 91
card verification value (CVV), 98
CATA. *See* Capital Area Transportation Authority (CATA)
Caterpillar, 148
CCE. *See* Certified Computer Examiner (CCE)
CCIE. *See* Cisco Certified Internetwork Expert (CCIE) certification
CCO. *See* chief compliance officer (CCO)
CCTV. *See* closed circuit TV cameras (CCTV)
CDA. *See* Communications Decency Act (CDA)
CDT. *See* Center for Democracy and Technology (CDT)
Ceglia, Paul, 48–49
cell phones, 159, 309
censorship on Internet, 188–189
Center for Democracy and Technology (CDT), 133
Center for Media Research, 139
Centers for Medicare and Medicaid Services, 310
Central Intelligence Agency (CIA), 146, 151
certification
  Cisco Systems, Inc., programs offered by, 57
  definition of, 57
  IBM, programs offered by, 57
  industry association, 58
  of information technology professionals, 57–58
  Microsoft, programs for, 57
  Oracle Corporation, programs for, 57
  SAP, North America, programs for, 57
  vendor, 57
Certified Computer Examiner (CCE), 113
Certified Information Systems Security Professional (CISSP), 113
Certified Software Development Associate (CSDA), 55
Certified Software Development Professional (CSDP) program, 55
Chambers, John, 1
charge-backs, 98
Chase Bank, 91, 243
ChefVille, 47
Chevron, 353
Chevy Volt, 265
Chicago Transit Authority (CTA), 157–158
chief compliance officer (CCO), 65
Chiffons, 222
Child Online Protection Act (COPA), 185, 195
Children's Internet Protection Act (CIPA), 187–188
Children's Online Privacy Protection Act (COPPA), 140, 185
children's personal data, 139–140
Chinese espionage, 219
CHIP. *See* Computer Hacking and Intellectual Property (CHIP) program
CIA. *See* Central Intelligence Agency (CIA)
Cincinnati Bell, 266–267
CIPA. *See* Children's Internet Protection Act (CIPA)
Cisco Certified Internetwork Expert (CCIE) certification, 57
Cisco Foundation, 2
Cisco Systems, Inc., 392
  certification programs of, 57
  ethical behavior at, 1–2
CISSP. *See* Certified Information Systems Security Professional (CISSP)
Citadel malware toolkit, 82
Citibank, 6, 94
CitiGroup, 5, 136
CityTime scandal, 41–43
CityVille, 47, 352
Civil Rights Act, Title VII of, 343
Clarke, Roger, 135
Classmate PC, 308–309
Classmate+, 308–309
ClearSail/Family.NET, 186
clients, professional relationships with, 47–50
closed circuit TV cameras (CCTV), 157
cloud computing, 85, 148
CMMI. *See* Capability Maturity Model Integration (CMMI)
CMMI-Development (CMMI-DEV), 273–274
Coca-Cola, 232, 341–342
Coca-Cola Conversations blog, 341
code of conduct, 392
  of information and communications technology, 392–393
  of Intel Corporation, 16–17, 392

code of ethics
corporate, 15–17
definition of, 15
of information technology professionals, 54
professional, 54
Software Engineering, 55–56
Code Red worm, 89, 109
coemployment relationship, 374
Cognizant Technology Solutions, 381
Coke, 46
Coke Secret Formula campaign, 341
collusion, 96
Comedy Central, 227
commercial software, vulnerability of, 87–88
Committee on Improving Cybersecurity Research, 100
common good approach, 24
Common Sense, 190
Communications Act, 141
Communications Assistance for Law Enforcement Act (CALEA), 143–146
Communications Decency Act (CDA), 184–185
Communications of the ACM, 55
community, 9
company-owned social networking Web Site, 342
company software, 63
Compaq, 381
competency, 60
competitive intelligence, 97, 239–241
complex computing, vulnerability of, 85–86
compliance, 64–66
computer and Internet crime, 81–114
bring your own device (BYOD) policies, 87
commercial software, vulnerability of, 87–88
complex computing, vulnerability of, 85–86
computer system risks, 86–87
computer user expectations, 86
exploits, 88–95
federal laws for, 99–100
information technology security incidents, 84–100
perpetrators, types of, 95–99
prevalence of, 84–88
trustworthy computing, implementation of, 100–114
computer/computing. *See also* trustworthy computing
cloud, 85, 148
exploits aimed at, 88
green, 390–392
low-cost, 307–309
process-control, 267
records on, 151
resources on, 62
risks in, 86–87
user expectations of, 86
computer forensics, 112–114
Computer Hacking and Intellectual Property (CHIP) program, 224
Computer Maintenance Competition Assurance Act, 226
Computing Research Association, 372
conduct, code of, 16–17, 392–393
Conficker worm, 89
confidential data, 62
conflict of interest, 48
consistency, 9–10
consumer data, 148, 155
consumer profiling, 154–155
Consumer Reports, 185
Content Scramble System (CSS), 226
contingent workers, 374–377
advantages of using, 375
definition of, 374
disadvantages of using, 375
at Microsoft, 376–377
use of, 376–377
contract, breach of, 49
contract workers, 105
contributory negligence, 269
Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, 90, 196–198
cookies, 154–155
COPA. *See* Child Online Protection Act (COPA)
COPPA. *See* Children's Online Privacy Protection Act (COPPA)
Copyright Act, 221, 225, 237
copyrighted material, 194
Copyright Office, 226
copyrights, 221–228
Agreement on Trade-Related Aspects of Intellectual Property Rights and, 224–225
definition of, 221
Digital Millennium Copyright Act and, 225–228
eligible works and, 222
fair use doctrine and, 222–223
General Agreement on Tariffs and Trade and, 224
infringement of, 221, 227–228
on intellectual property, 221–228
Prioritizing Resources and Organization for Intellectual Property Act and, 224
software copyright protection and, 223–224
terms of, 221–222
World Intellectual Property Organization and, 225
World Trade Organization and, 224–225
Copyright Term Extension Act, 221–222
CORI database, 241

corporate compliance officer, 13–14
corporate ethics, 12–18
  by board of directors, 14–15
  Code of Ethics and, 15–17
  corporate ethics officer and, 13–14
  ethics appraisals and, 18
  ethics training and, 17–18
  social audits and, 17
corporate ethics officer, 13–14
corporate firewall, 63–64, 105–106
Corporate Responsibility, 16–17
corporate social responsibility (CSR), 8–12
  business practices and, 10–11
  in community, 9
  consistency and, 9–10
  fostering, 8–12
  legal action and, 11
  publicity and, 11–12
Countrywide Financial, 5
Coursea, 235
Coverity, 266
crackers, 96
credit card fraud, 98
crime. *See also* computer and Internet crime
  in online virtual worlds, 352–353
criticality, 280
cross-licensing agreements, 231
Crunchbase database, 240
CSDA. *See* Certified Software Development Associate (CSDA)
CSDP. *See* Certified Software Development Professional (CSDP) program
CSFA. *See* CyberSecurity Forensic Analyst (CSFA)
CSR. *See* corporate social responsibility (CSR)
CSS. *See* Content Scramble System (CSS)
CTA. *See* Chicago Transit Authority (CTA)
customer service, 343–344
CVV. *See* card verification value (CVV)
Cyber Angels, 347
cyberbullying, 346–347
cybercriminals, 98–99
CyberSecurity Forensic Analyst (CSFA), 113
CyberSource Corporation, 7
cybersquatters/cybersquatting, 243
cyberstalking, 347–348
cyberterrorism, 108–109
cyberterrorists, 99

D

Dallas Independent School District (DISD), 298–299
data
  breaches of, 98, 151–153
  children's personal, 139–140
  confidential, 62
  consumer, 148, 155
  financial, 135–137
  personal, 139–140
  privacy rights and, 148
  private, 62
  protection of, 62
database administrator (DBA), 60
Data Processing Management Association, 56
Data Protection Directive, 148
DBA. *See* database administrator (DBA)
DDoS. *See* distributed denial-of-service (DDoS) attacks
decision making, 20–24. *See also* alternative decision making
  ethical, 20–24, 54
  implementation of, 24
  problem statement, 21
  results of, 24
decision support system (DSS), 267
Declaration of Independence, 190
decompilers, 237
DeCSS, 226
defamation
  Facebook, lawsuits against, 184–185
  First Amendment and, 183
  Twitter, lawsuits against, 184–185
DEFCON, 96
deliverables, 265
Dell
  code of conduct of, 392
  customer service and, 344
  green computing and, 391
  IdeaStorm, 342
  social networking Web site for, 342
Deloitte, 370
Delta, 65
Denault, Gerald, 42–43
Design Criteria Standard for Electronic Management Software applications (DoD 5015), 64–65
detection, 110
detection rating, 280
Dex One Corporation, 384
DHS. *See* U.S. Department of Homeland Security (DHS)
Diamond v. Diehr, 230
Dibon Solutions, 380–381
digital divide, 306–310
  definition of, 306
  Education Rate program, 307
  low-cost computers and, 307–309
  mobile phones and, 309–310
Digital Millennium Copyright Act (DMCA), 225–228

direct advertising, 340
Directive 95/46/EC. *See* European Union Data Protection Directive (Directive 95/46/EC)
DISD. *See* Dallas Independent School District (DISD)
Disneyland, 276
distributed denial-of-service (DDoS) attacks, 91–92
DMCA. *See* Digital Millennium Copyright Act (DMCA)
DoD 5015. *See* Design Criteria Standard for Electronic Management Software applications (DoD 5015)
Doe v. Holder, 146
Doe v. 2TheMart.com, Inc., 193
DOL. *See* U.S. Department of Labor (DOL)
Domain Awareness system, 158
"Do Not Track" button, 154
Dow Jones Industrial, 262
doxing, 191
DreamHost, 110
drive-by malware, 82
Droid®, 302
DSS. *See* decision support system (DSS)
due diligence, 370
Dun & Bradstreet, 240
DuPont, 219, 233
duty of care, 60–61
dynamic testing, 272
DYVINE system, 157

E

Eagle School District, 298
Earth Link, 192
eBay, 94, 336
EBITDA (earnings before interest payments, taxes, depreciation, and amortization), 369
ECN. *See* European Counter Network (ECN)
e-commerce, 148
Economic Espionage Act of 1996, 97
ECPA. *See* Electronic Communications Privacy Act (ECPA)
e-discovery. *See* electronic discovery (e-discovery)
EDRs. *See* event data recorders (EDRs)
Education Rate (E-Rate) program, 187, 297–300, 307
EFF. *See* Electronic Frontier Foundation (EFF)
EHRs. *See* electronic health records (EHRs)
EICC. *See* Electronic Industry Citizenship Coalition (EICC)
Eldred, Eric, 222
Eldred v. Ashcroft, 222
eLearn, 55
electronically stored information (ESI), 153–154
electronic communication, 143
Electronic Communications Privacy Act (ECPA), 142–143, 191
Electronic Data Systems, 381
electronic discovery (e-discovery), 153–154
Electronic Frontier Foundation (EFF), 133, 185, 193
electronic health records (EHRs), 310–314
Electronic Industry Citizenship Coalition (EICC), 392–393
Electronic Privacy Information Center, 135, 185
Electronic Product Environmental Assessment Tool (EPEAT), 391
electronic surveillance, 140–146
  Communications Act, 141
  Communications Assistance for Law Enforcement Act, 143–146
  Electronic Communications Privacy Act, 142–143
  Foreign Intelligence Surveillance Act, 141, 146
  Omnibus Crime Control and Safe Streets Act, Title III of the, 141–142
  US Department of Justice, requests of, 141
Electronic Waste Recycling Act, 391
Eleventh Circuit Court of Appeals, 195
eligible works, 222
Ellison, Larry, 387
email, 90–91, 104
Emarketer, 338
employees/employers
  ethics training, requirement of, 17–18
  leasing of, 374
  professional, 44
  professional relationships with, 45–47
  trade secrets and, 233–234
  trustworthy computing, education on, 105
EnCE Certified Examiner program, 113
Engineering Registration Act, 58–59
Enron, 6, 15
enterprise resource planning (ERP) systems, 59, 374
Entropia Universe, 352
EPEAT. *See* Electronic Product Environmental Assessment Tool (EPEAT)
ePhoneTracker, 159
Equifax, 137
eradication, 111
E-Rate. *See* Education Rate (E-Rate) program
ERC. *See* Ethics Resource Center (ERC)
ERP. *See* enterprise resource planning (ERP) systems

ESI. *See* electronically stored information (ESI)
espionage
  Chinese, 219
  industrial, 97, 240
ethical behavior, 1–2, 54
ethical decision making, 54
ethical work environment, 18–19
ethics. *See also* code of ethics
  appraisals on, 18
  business, 5–19
  corporate, 12–18
  decision making and, 20–24, 54
  definition of, 3–4
  information technology, 24–25, 61–64, 369–393
  integrity, importance of, 4
  of Intel Corporation, 16
  laws and, 5
  morals and, 5
  at Motorola, training of, 18
  organizational (*See* information technology (IT) organizational ethics)
  overview of, 1–25
  social networking and, 345–351
  training on, 17–18
Ethics Policy, 104
Ethics Resource Center (ERC), 12–13, 17–18
European Commission, 148
European Counter Network (ECN), 192
European Data Protection Regulation, 148
European Union Data Protection Directive (Directive 95/46/EC), 147–148
European Union's Restriction of Hazardous Substances Directive, 391
evaluation benchmark, 54
event data recorders (EDRs), 158–159
evidence, 111
Excel, 236
Experian, 137, 148
exploits, 88–95. *See also* security
  on Android, 88
  definition of, 87
  distributed denial-of-service attacks, 91–92
  of H-1B workers, 380–381
  phishing, 93–94
  rootkits, 92–93
  on smartphones, 88
  smishing, 94–95
  spam, 90–91
  Trojan horses, 89–90
  types of, 88–95
  viruses, 89
  vishing, 94–95
  worms, 89
Explorer, 154
expression
  anonymous, 190
  freedom of, 179–198

F

Facebook
  Coca-Cola on, 341–342
  consumer data on, 148
  customer service and, 344
  defamation lawsuits, 184–185
  doxing on, 191
  fraud against, 48–49
  hiring process and, 342
  inappropriate material on, 350
  indirect advertising on, 341
  initial public offering of, 263
  John Doe lawsuits against, 192
  violating terms of service for, 343
  workplace monitoring of, 155
failure mode, 280
failure mode and effects analysis (FMEA), 280
Fair and Accurate Credit Transactions Act, 137
Fair Credit Billing Act, 98
Fair Credit Reporting Act, 136–137
fair information practices, 146–148
fairness approach, 23
fair use doctrine, 222–223
False Claims Act, 386–387
Family Educational Rights and Privacy Act (FERPA), 139–140
Fannie Mae, 5
FarmVille, 352
Favre, Bret, 196
FBI. *See* Federal Bureau of Investigation (FBI)
FCC. *See* Federal Communications Commission (FCC)
FCPA. *See* Foreign Corrupt Practices Act (FCPA)
Federal Bureau of Investigation (FBI), 81–82, 95
  National Security Letter issued by, 146
  trade secrets and, 233
Federal Communications Commission (FCC), 141, 143, 297, 299
federal laws, for computer and Internet crime, 99–100
Federal Register, 150
Federal Rules of Procedure, 153
Fen-Phen, 10
FERPA. *See* Family Educational Rights and Privacy Act (FERPA)
F-14 fighter jet, 279
filtering on Internet, 185–186

financial data, 135–137
Fair and Accurate Credit Transactions Act, 137
Fair Credit Reporting Act, 136
Gramm-Leach-Bliley Act, 136–137
Right to Financial Privacy Act, 136
Financial Privacy Rule, 137
Financial Services Modernization Act, 136–137
Firefox, 154
Firestone, 278
firewall, corporate, 63–64
First Amendment, 181–183
adoption of, 181
anonymous speech right, 193
children's personal data, regulations of, 139
defamation and, 183
definition of, 181–182
freedom of expression and, 181–183
NSL gag provision, violation of, 146
obscene speech and, 183
pornography, 194
social networks and, 349
US Supreme Court, interpretation by, 182, 184
first-inventor-to-file system, 230
first-to-invent system, 230
FISA. *See* Foreign Intelligence Surveillance Act (FISA)
FlexiSPY, 159
FMEA. *See* failure mode and effects analysis (FMEA)
FOIA. *See* Freedom of Information Act (FOIA)
Ford, 148, 268, 278
Foreign Corrupt Practices Act (FCPA), 6, 51, 65
foreign intelligence, 141
Foreign Intelligence Surveillance Act (FISA), 141–142, 146
Fourth Amendment, 141–142
advanced surveillance technology, 157
civil liberties under, 132
privacy rights under, 132, 134
unreasonable government searches, 156
Fox News Channel, 15
fraud, 48
credit card, 98
against Facebook, 48–49
Freddie Mac, 5
freedom of expression, 179–198
anonymity on Internet and, 190–193
Child Online Protection Act and, 185
Children's Internet Protection Act and, 187–188
Communications Decency Act and, 184–185
First Amendment rights and, 181–183
hate speech and, 193–194
information on Internet and, 184–189
on Internet, 185–186, 188–189
pornography and, 194–198
strategic lawsuit against public participation and, 189–190
Freedom of Information Act (FOIA), 149–150
Free Expression Policy Project, 185
FrontierVille, 47
FTC. *See* U.S. Federal Trade Commission (FTC)
Fuhu, 232
Fukushima Daiichi Nuclear Power Plant, 277

G

G20. *See* Group of 20 (G20)
GAAP. *See* generally accepted accounting principles (GAAP)
GAO. *See* General Accounting Office (GAO)
Gap Inc., 148
Gartner Group, 382
GATT. *See* General Agreement on Tariffs and Trade (GATT)
GCFA. *See* Global Information Assurance Certification Certified Forensics Analyst (GCFA)
GDP. *See* gross domestic product (GDP)
General Accounting Office (GAO), 299–300
General Agreement on Tariffs and Trade (GATT), 224
General Electric, 381
generally accepted accounting principles (GAAP), 66
General Services Administration (GSA), 49, 387
Georgia Powerball, 265
gifts, 51–52
Glass-Steagall law, 136
GLBA. *See* Gramm-Leach-Bliley Act (GLBA)
Global Crossing, 15
Global Hunger Relief Program, 2
Global Information Assurance Certification Certified Forensics Analyst (GCFA), 113
Global Services Location Index, 382
GM, 344
GNU General Public License (GPL), 239
Gomez, Selena, 140
good business ethics, importance of, 8–12
Google. *See also* Android
Bing search engine by, 236
Chinese espionage by, 219
consumer data on, 148
copyright infringement lawsuit against, 227
creating account on, 194
email service offered by, 90
European Data Protection Regulation and, 148
HathiTrust Digital Library project, 223

noncompete agreements with, 234
patent infringement claims by, 231
social responsibility activities of, 12
US Federal Trade Commission, investigation by, 12
government licensing
definition of, 58
of information technology professionals, 58–60
legislation established for, 59–60
government records
access to, 148–151
Freedom of Information Act, 149–150
Privacy Act, 151
government searches, unreasonable, 156
GPL. *See* GNU General Public License (GPL)
Gradiente iPhone, 242
Grady Memorial Hospital, 384
Gramm-Leach-Bliley Act (GLBA), 136–137
green computing, 390–392
Apple and, 391
definition of, 372
Dell and, 391
Hewlett-Packard Company and, 391
"green PC," 390
Greenpeace ratings, 392
gross domestic product (GDP), 301
gross mismanagement, 387
group advertising, 341–342
Group of 20 (G20), 51
groups on social networking, 341–342
Grum botnet, 92
GSA. *See* General Services Administration (GSA)
GTSI Corporation, 11
Guidance Software, 113
Guidelines for the Protection of Privacy and Transborder Flows of Personal Data, 147
Guyton, Odell, 14

H

hackers, 96
hacktivists, 99
Hangover IV, 340
Happy Farm, 352
Harper, Gloria, 298
Harrison, George, 222
hashtags, 335
hate speech, 193–194
HathiTrust Digital Library project, 223
hazard log, 276
healthcare
American Recovery and Reinvestment Act, 139
costs of, 310–318
electronic health records (EHRs) and, 310–314
Health Insurance Portability and Accountability Act, 138–139
information on, 138–139
medical information Web sites and, 317–318
mobile technology and, 314–315
telehealth and, 315–317
wireless technology and, 314–315
Health Information Technology for Economic and Clinical Health Act (HITECH), 139, 151–152, 312–314
Health Information Trust Alliance, 152
Hewlett-Packard Company (HP), 298–299, 369–371
code of conduct of, 392
green computing and, 391
HGL Technologies, 384
high-frequency trading, 261
high-quality software systems, 264
HIPAA. *See* U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Hippocratic oath, 54
hiring process, 342–343
HISD. *See* Houston Independent School District (HISD)
HITECH. *See* Health Information Technology for Economic and Clinical Health Act (HITECH)
Homeland Security and Emergency Management Agency (HSEMA), 157
H-1B workers, 377–381
application process for, 379–380
exploitation of, 380–381
US workers *vs.*, 380
visa of, 47
Hotmail, 342
House Armed Services subcommittee on Emerging Threats and Capabilities, 133
Houston Independent School District (HISD), 298–299
Howard v. Miami Twp, Fire Div, 158
HP. *See* Hewlett-Packard Company (HP)
HSEMA. *See* Homeland Security and Emergency Management Agency (HSEMA)
HTC, 231
HTML. *See* Hypertext Markup Language (HTML)
Hypertext Markup Language (HTML), 112

I

IAEA. *See* International Atomic Energy Agency (IAEA) network

IBM
business ethics of, 6
certification programs of, 57
code of conduct of, 392
consumer data and, 148
outsourcing and, 381
patents obtained by, 229
ICANN. *See* Internet Corporation for Assigned Names and Numbers (ICANN)
ICD-10, 311
ICT. *See* information and communications technology (ICT)
IC3. *See* Internet Crime Complaint Center (IC3)
IdeaStorm, 342
IDOL. *See* Intelligent Data Operating Layer (IDOL)
IDS. *See* intrusion detection system (IDS)
IEEE. *See* Institute of Electrical and Electronics Engineers (IEEE)
IEEE-CS. *See* Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS)
IGB Eletronica, 242
ILOVEYOU worm, 89
inappropriate material, 350–351
incidents
containment of, 111
follow-up on, 111–112
involving security, 84–100
notification of, 110
reporting, 111–112
indirect advertising, 341–342
individual network of friends, 340–341
industrial espionage, 97, 240
industrial spies, 97
industry association certification, 58
information and communications technology (ICT), 372
code of conduct of, 392–393
information privacy, 135
Information Protection Assessment kit, 109
information sensitivity policy, 104
information sharing, 62
information systems, 63
information technology (IT), 297–318
ethics in, 24–25
on healthcare costs, 310–318
productivity and, 301–303
security and, 84–100
on standard of living and work productivity, 301–310
information technology (IT) investment, 301–303
productivity and, 301–305
telework and, 304–305
information technology (IT) organizational ethics, 369–393
contingent workers and, 374–377
green computing and, 390–392
H-1B workers and, 377–381
information and communications technology, code of conduct of, 392–393
issues concerning, 371–373
nontraditional workers and, 372–373
outsourcing and, 381–385
whistle-blowing and, 385–390
information technology (IT) professionals, 43–61
certification of, 57–58
code of ethics of, 54
government licensing of, 58–60
malpractice by, 60–61
organizations and, 55–56
professionalism of, 44
professional services industry and, 43–44
relationships with, 44–54
information technology (IT) users, 61–66
company software for, 63
compliance of, 64–66
computer resources of, 62
corporate firewall for, 63–64
definition of, 53
ethical issues for, 61–62
ethical practices of, 63–64
information systems and, 63
professional relationships with, 53
resources for, 63
sharing of information by, 62
software piracy by, 61
information technology (IT) workers. *See* information technology (IT) professionals
Infosys, 47
infringement
of copyrights, 221, 227–228
of patents, 153, 230–231
initial public offering (IPO), 262–263
Institute of Electrical and Electronics Engineers (IEEE), 55–56
Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS), 55–56
integration testing, 273
integrity, importance of, 4
Intel Corporation
Business Software Alliance membership of, 46
code of conduct of, 16–17, 392
Corporate Responsibility Report of, 17
ethical performance of, 16
noncompete agreements with, 234
trade secrets of, 46
Intel Learning Series Software Suite, 309
intellectual property (IP), 217–243
competitive intelligence and, 239–241
copyrights on, 221–228

cybersquatting and, 243
defined, 220
issues with, 234–243
open source code and, 238–239
patents on, 228–231
plagiarism and, 234–236
reverse engineering and, 236–238
trademark infringement and, 242
trade secrets and, 231–234
intelligence
competitive, 97, 239
foreign, 141
Intelligent Data Operating Layer (IDOL), 369
intentional misrepresentation, 270
Internal Revenue Code, 140
Internal Revenue Service (IRS), 265, 376
internal whistle-blowing, 388
International Atomic Energy Agency (IAEA) network, 99
International Organization for Standardization (ISO), 279
Internet
anonymity on, 190–193
censorship on, 188–189
crime on (*See* computer and Internet crime)
filtering of, 185–186
freedom of expression on, 184–189
security threats on, 109
Internet Corporation for Assigned Names and Numbers (ICANN), 243
Internet crime. *See* computer and Internet crime
Internet Crime Complaint Center (IC3), 81–83
InternetSafety.com™, 186
Internet service providers (ISPs), 90, 186, 192, 194
safe harbors for, 226–227
intrusion detection system (IDS), 106–107, 110
Intuit, 234
investment, information technology, 301–303
IP. *See* intellectual property (IP)
iPad®, 7, 50, 342, 391
iParadigms, 235
iPayments, 234
iPhone®, 7, 49, 50, 88, 186, 223, 233, 238, 242, 302
iPod®, 50, 223
IRS. *See* Internal Revenue Service (IRS)
ISO. *See* International Organization for Standardization (ISO)
ISO 9001 family of standards, 279–280
ISPs. *See* Internet service providers (ISPs)
IT. *See* information technology (IT)
iThenticate, 235
iTouch®, 223
iTunes, 223

J

Jacobs, John, 352
Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act, 349
Java, 83, 87, 231
Jet Blue, 344
John Doe lawsuits, 192–193, 227
Joint Commission on Accreditation of Healthcare Organizations, 315
Joint Steering Committee for the Establishment of Software Engineering as a Profession, 55
Journal News, The, 150
JPMorgan Chase, 136

K

Kaiser Family Foundation, 185
Karabasevic, Dejan, 219
Kaspersky Internet Security 2012, 107–108
Kaspersky Labs, 85, 90
Katz v. United States, 141, 156
Kaushik, Avinash, 240
Kennedy, President, 149
keystroke monitoring, 156–157
KFC, 46
Kibbe, David, 314
kickbacks, 50
Kixeye, 47
Knight Capital, 263
knowledge-based intrusion detection system, 106
Kohlberg, Lawrence, 17
KPMG, 370

L

Labor Condition Application (LCA), 379–380
labor productivity growth rates, 303
lamers, 96
Lanham Act, 242
laws
anti-SLAPP, 190
for computer and Internet crime, 99–100
ethics and, 5
federal, 99–100
Glass-Steagall, 136
privacy, 133–151
for trade secrets, 232–233
LCA. *See* Labor Condition Application (LCA)

Leahy-Smith America Invents Act, 230
leasing firm, 374
legal action, 11
Lehman Brothers, 5, 15
L'Enfant Plaza station, 276
Lenovo, 392
liability
  product, 268–275
  strict, 268–269
libel statement, 183
licensing, 58–60
Lincoln Law, 386
LinkedIn, 155, 342
Linux, 308, 309
live telemedicine, 316
Lockheed Martin, 94, 219
logic bomb, 90
Lovato, Demi, 140
low-cost computers, 307–309
Lucasfilm, 234
Lucile Packard Children's Hospital, 152
Lumina 900 smartphone, 265
Lynch, Michael, 370–371

M

M. A. Mortenson Company, 270
MAA. *See* Machine Accountants Association (MAA)
Machine Accountants Association (MAA), 56
Macintosh user interface of Apple, 236
Mack, Ronald, 222
Madoff, Bernard, 5
malicious insiders, 96–97, 108
malpractice, 60–61
malware, 82, 88
Manning, Bradley, 7
Mariner I space probe, 275
Market Web Site for Android, 61
Marshalls, 390
massively multiplayer online game (MMOG), 352
massive multiplayer online role-playing games (MMORPG), 352
MasterCard, 98, 390
material breach of contract, 49
Math Works, The, 46
McAfee, 46, 107, 186
McGahn, Daniel, 217–218, 220
MCI, 41
"Mean Joe Greene—The Making of the Commercial," 341
Medicaid, 313
medical information websites, 317–318
medical records, 138
Medicare, 313
Melissa worm, 89
Mformation, 231
Microsoft
  Business Software Alliance membership of, 46
  certification programs of, 57
  code of conduct of, 392
  consumer data and, 148
  contingent works used by, 376–377
  email service offered by, 90
  Excel, 236
  Internet filtering on smartphones, 186
  operating systems of, 266
  outsourcing and, 381
  trustworthy computing, initiative implemented by, 100–101
  unlicensed use of, 46
  Windows, 83, 266, 309, 382
  Word, 93, 236
Miller, Marvin, 183
Miller v. California, 183, 195
Minecraft, 352
Mino, 223–224
misrepresentation, 49
Missile Defense Agency, 62
MMOG. *See* massively multiplayer online game (MMOG)
MMORPG. *See* massive multiplayer online role-playing games (MMORPG)
Mobile Nanny, 159
mobile phones, 309–310
Mobile Spy, 159
mobile technology, 314–315. *See also* specific types of
MoneyPak, 82
moral code, 3
morality, 3
morals, 5
Morgridge, Emeritus John, 2
Motorola, 18, 231, 381
MTV, 227
Murdoch, Rupert, 15
MySpace, 155, 343
  inappropriate material on, 350
  sexual predators on, 348–349

N

Nabi, 232
Narus, 132
NASDAQ stock exchange, 16, 263

National Academy of Sciences, 100
National Association for the Advancement of Colored People (NAACP) v. Alabama, 191
National Association of Criminal Defense Lawyers, 11
National Association of Manufacturers, 11
National Business Ethics Survey, 13, 17
National Campaign to Prevent Teen and Unplanned Pregnancy, 196
National Center for Victims of Crime, 348
National Council of Examiners for Engineering and Surveying (NCEES), 59–60
National Fraud Alert system, 137
National Highway Traffic Safety Administration (NHTSA), 158
National Oncology Institute, 275
National School Lunch Program, 307
National Security Agency (NSA), 131–133, 219
National Security Letter (NSL), 142, 146
National Whistleblowers Center, 389
National White Collar Crime Center, 81
NCEES. *See* National Council of Examiners for Engineering and Surveying (NCEES)
Negev Nuclear Research Center, 99
negligence, 60–61, 269
negligent insiders, 97
Neighborhood Watch, 191
Net Nanny Parental Controls, 186
NetZero/Juno, 192
Neverdie (avatar character), 352
New Media Consortium (NMC), 353
News Corporation scandal, 15
New Scotland Yard, 157
News International Ltd., 15
News of the World, 15
Newtown school shooting, 150
New York State Association of Criminal Defense Lawyers, 11
New York Stock Exchange, 263
New York Times, 133, 146
New York University, 379
NHTSA. *See* National Highway Traffic Safety Administration (NHTSA)
Nielsen survey, 195
Nintendo, 223, 352
Ninth Circuit Court of Appeals, 195, 242
NMC. *See* New Media Consortium (NMC)
Nokia, 265, 382
nominative fair use, 242
noncompete agreements, 233–234
nondisclosure clauses, 233
nonobviousness, 229
nontraditional workers, 372–373
Northrop Grumman, 275
Norton AntiVirus antivirus software, 107
Norton Online Living, 139
novelty, 229
NSA. *See* National Security Agency (NSA)
NSL. *See* National Security Letter (NSL)
NSS Labs, 108
N-version programming, 277–278
NYSE, 16

O

obscene speech, 183
OCC. *See* Office of the Comptroller of the Currency (OCC)
occurrence rating, 280
OCR. *See* Office for Civil Rights (OCR)
OECD. *See* Organisation for Economic Co-operation and Development (OECD)
Office for Civil Rights (OCR), 139
Office of Inspector General, 299
Office of the Comptroller of the Currency (OCC), 6
Office of the National Counterintelligence Executive, 233
Office of the United States Intellectual Property Enforcement Representative, 224
offshore outsourcing, 381–383. *See also* outsourcing
OLED. *See* Organic Light Emitting Diodes (OLED)
OLPC. *See* One Laptop per Child (OLPC)
OLPC XO, 308
Omnibus Crime Control and Safe Streets Act, Title III of the, 141–142
One Laptop per Child (OLPC), 307–308
Online Copyright Infringement Liability Limitation Act, 226
online credit card fraud, 98
online paper mills, 234
online reputation management companies, 179–181
online social networking, 338–345
online virtual worlds, 351–353
  business uses of, 353
  crime in, 352–353
  definition of, 351
  educational uses of, 353
open source code, 238–239
Open Source Initiative (OSI), 239
Open Table, 65
opt in, 137
opt out, 137

Oracle Corporation
breach of contract by, 49
certification programs of, 57
code of conduct of, 392
False Claims Act and, 387
Java, 83, 87, 231
patent infringement claims by, 231
vulnerabilities of software of, 87
whistle-blowing at, 387
Organic Light Emitting Diodes (OLED), 233
Organisation for Economic Co-operation and Development (OECD), 147
organizational ethics. *See* information technology (IT) organizational ethics
organizations
information technology professionals and, 55–56
professional, 55–56
OSI. *See* Open Source Initiative (OSI)
outsourcing, 303, 381–385
cons of, 383–384
definition of, 381
IBM and, 381
Microsoft and, 381
offshore, 381–383
pros of, 383–384
strategies for successful, 384–385

P

Paine, Thomas, 190
Palm, 238
Paramount Pictures, 227
Parastoo, 99
patents, 228–231
cross-licensing agreements and, 231
definition of, 228
IBM, obtained by, 229
infringement of, 153, 230–231
on intellectual property, 228–231
Leahy-Smith America Invents Act and, 230
software, 230–231
US Supreme Court and, 229
payoff, 50
PayPal, 94
PDAs. *See* personal digital assistants (PDAs)
pen register, 142–143
Pepsi, 148
Perella Weinberg, 371–372
permatemps, 376
perpetrators
crackers, 96
cybercriminals, 98–99
cyberterrorists, 99
hackers, 96
hacktivists, 99
industrial spies, 97
malicious insiders, 96–97
types of, 95–99
personal communication devices and voice-mail policy, 104
personal data, children's, 139–140
personal digital assistants (PDAs), 314–315
Personal Firewall antiviurs software, 107
phishing, 93–94
phones. *See also* smartphones
cell, 159, 309
mobile, 309–310
Pinterest, 192
Pixar, 234
plagiarism, 234–236
Playboy, 242
Playboy Enterprises, Inc. v. Terri Welles, 242
Playboy™ Playmate of the Year™, 242
Playmate of the Year, 242
pornography, 62, 194
Controlling the Assault of Non-Solicited Pornography and Marketing Act for, 196–198
freedom of expression and, 194–198
pornography purveyors, 195
PPLS. *See* Pre-Paid Legal Services (PPLS)
Pregnancy Discrimination Act, 343
Pre-Paid Legal Services (PPLS), 193
Pre-Paid Legal v. Sturtz et al, 193
Pretexting Rule, 137
prevention, trustworthy computing and, 105–109
PricewaterhouseCoopers LLP Health Research Institute, 312–313
prior art, 229
Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act, 224
privacy, 131–159. *See also* anonymity
application of, 135–151
consumer data, 155
court rulings and, 135–151
Fourth Amendment, rights under, 132, 134
information, 135
laws on, 133–151
protecting of, 133–151
reasonable expectation of, 134, 156
right of, 135
US Supreme Court, concept of, 134
Privacy Act, 151
Privacy Protection Study Commission, 135
private data, 62
private-sector workers, 387
problem statement, 21
process-control computers, 267
Procter & Gamble, 148

productivity
defined, 301
information technology and, 301–305
product liability
definition of, 268
of software, 268–275
profession, defined, 43
professional code of ethics, 54
professional education programs, 60
professional employee, 44
professionalism, 44
professional negligence, 61
professional organizations, 55–56. *See also* information technology (IT) organizational ethics
Association for Computing Machinery, 55–56
Association of Information Technology Professionals, 56
Institute of Electrical and Electronics Engineers Computer Society, 55–56
SysAdmin, Audit, Network, Security Institute, 56
professional relationships, 53
with clients, 47–50
with employees/employers, 45–47
with information technology users, 53
management of, 44–54
with other professionals, 52–53
within society, 53–54
with suppliers, 50–52
professionals. *See also* information technology (IT) professionals
professional relationships with other, 52–53
professional services industry, 43–44
profiling, consumer, 154–155
PRO-IP. *See* Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act
Protected Critical Infrastructure Information Program, 108
publicity, 11–12
public respect and trust, 54
Pythagoras, 229

Q

QA. *See* quality assurance (QA)
Qantas, 268
quality assurance (QA), 272, 276–277
quality management, 265
software, standards for, 279–281
Quicken tax preparation software, 381
qui tam, 386
Qwest, 15

R

RAID. *See* redundant array of independent disks (RAID)
RAND Corporation, 313–314
ransomware, 81–82
Rapportive software, 240
Raspberry Pi, 309
Raspberry Pi Foundation, 309
Raytheon, 280
reasonable assurance, 103
reasonable expectation of privacy, 134, 156
reasonable person standard, 60
reasonable professional standard, 60
REC. *See* Reverse Engineering Compiler (REC) decompiler
redundancy, 277
redundant array of independent disks (RAID), 277
Reg NMS. *See* Regulation National Market System (Reg NMS)
Regulation National Market System (Reg NMS), 261
regulations, 303
reliability, defined, 278
remote monitoring, 316
Reputation Changer, 180
Research In Motion, 231
BlackBerry®, 88, 238, 302
respondeat superior, 11
résumé inflation, 52–53
reverse engineering, 236–238
Reverse Engineering Compiler (REC) decompiler, 237
Reveton ransomware attack, 82–83
Right to Financial Privacy Act, 136
Rihanna, 140
risk, defined, 277
risk assessment policy, 102–104
risk priority rating, 280
RISKS Forum, 55
Rockefeller, John D., 297–298, 300
rootkit virus, 92–93
Royal Air Force, 275
Rutgers, 346

S

Safari, 12, 154
Safe Eyes®, 186
Safeguards Rule, 137
safety-critical system, 275–279
SAIC. *See* Science International Applications Incorporated (SAIC)

Samsung, 153, 231, 392
San Jose Public Library, 185
SANS. *See* SysAdmin, Audit, Network, Security (SANS) Institute
Santa Clara County Superior Court, 193
SAP, North America, 57
Sarbanes-Oxley Act of 2002, 385
  compliance with, 65
  passing of, 15–16
SAS. *See* Statement on Auditing Standards (SAS)
Satyam Computer Services, 5
Saudi Arabian Oil Company (Aramco), 96
SBA. *See* Small Business Administration (SBA)
Schools and Libraries Program of the Universal Service Fund, The, 307
Science International Applications Incorporated (SAIC), 41–43
script kiddies, 96
SC 13D acquisition, 240
SCVNGR. *See* social location-based gaming platform for mobile phones (SCVNGR)
SEC. *See* U.S. Securities and Exchange Commission (SEC)
Second Circuit Court of Appeals, 146, 228
Second Life Education Microsites, 353
Second Life virtual world, 341, 352
Second Life Work Microsites, 353
security. *See also* exploits
  attacks on, 112
  audits of, 109
  federal laws for, 99–100
  incidents of, 84–100
  information technology and, 84–100
  perpetrators, 95–99
  prevalence of, 84–88
  trustworthy computing and policy on, 104–105
Sega, 237
Sega Enterprises Ltd. v. Accolade, Inc., 237
Senate Commerce Committee, 297
Senate Judiciary Committee, 159
Sensata Technology, 65
Sensis® Consumer Report, 304
severity rating, 280
Sex Offender Registration and Notification Provisions (SORNA), 349–350
sexting, 196
sexual predators, 348–350
sharing of information, 62
Shell, 381
Short Message Service (SMS) texting, 94, 315
SIGs, seespecial–interest groups (SIGs)
Sinovel Wind Group, 218–219
SirCam worm, 89
Siri intelligent assistant, 49, 231
Slammer worm, 109
SLAPP. *See* strategic lawsuit against public participation (SLAPP)
Slater & Gordon, 268
Small Business Administration (SBA), 11
smart cards, 98–99, 148
smartphones, 310
  exploits aimed at, 88
  Lumina 900, 265
  malware on, 88
  massively multiplayer online games on, 352
smishing, 94–95
SMS. *See* Short Message Service (SMS) texting
social audits, 17
social location-based gaming platform for mobile phones (SCVNGR), 341
social networking, 335–353
  advertising and, 339–342
  customer service, for improving, 343–344
  cyberbullying and, 346–347
  cyberstalking and, 347–348
  ethical issues with, 345–351
  First Amendment and, 349
  groups on, 341–342
  hiring process, use of, 342–343
  inappropriate material on, 350–351
  online, 338–345
  online virtual worlds on, 351–353
  sexual predators on, 348–350
  Social shopping Web sites and, 344–345
  US Department of Justice and, 343
  Web Sites for, 337–338, 342
social responsibility activities, 12
social shopping Web sites, 335–336, 344–345
society, professional relationships within, 53–54
Society for the Prevention of Cruelty to Animals (SPGA), 351
software, 261–281
  antivirus, 107
  AutoCAD, 97
  Capability Maturity Model Integration, 273–275
  CAPTCHA, 91
  commercial, vulnerability of, 87–88
  company, 63
  copyright protection for, 223–224
  defects of, 264–265
  development process for, 270–273
  issues in, 275–281
  patents for, 230–231
  piracy of, 4, 61
  product liability of, 268–275
  quality management standards for, 279–281
  quality of, 264–268

Quicken tax preparation, 381
Rapportive, 240
safety-critical system, development of, 275–279
spy, 159
testing, 272–273
virtualization, 86
Software Engineering Code of Ethics, 55–56
Software Engineering Institute at Carnegie Mellon, 273–274
Sonny Bono Copyright Term Extension Act, 221–222, 224
Sony Music Entertainment, 148, 392
Sony PlayStation, 223, 352
SORNA. *See* Sex Offender Registration and Notification Provisions (SORNA)
spam, 90–91
spear-phishing, 94
special-interest groups (SIGs), 55
speech
anonymous, 193
defined, 182
hate, 193–194
obscene, 183
SPGA. *See* Society for the Prevention of Cruelty to Animals (SPGA)
Spherion Atlantic Enterprises, 41–42
Sprint, 381
spy software, 159
stakeholder, 9
stalking app, 159
standard of living and work productivity, 301–310
digital divide on, 306–310
information technology investment and, 301–305
information technology on, 301–310
Standard & Poor 500, 262
standards of practice, 54
Stanford Achievement Test, 307
Stanford University, 152
Statement on Auditing Standards (SAS), 385
static testing, 273
store-and-forward telemedicine, 315–316
Stored Communications Act, 142
Storm worm, 89
Strategic and Competitive Intelligence Professionals organization, 241
Strategic Forecasting (Stratfor), 94
strategic lawsuit against public participation (SLAPP), 189–190
strict liability, 268–269
Stuffpit, 344–345
subscribing firm, 374
suicide, 346
suppliers, professional relationships with, 50–52
supply chain sustainability, 8
surveillance
advanced, 157–159
camera, 157–158
electronic, 140–146
Symantec, 46, 82, 107, 112
Symbian mobile operating system, 382
Syncapse, 341
Syntel, 383
SysAdmin, Audit, Network, Security (SANS) Institute, 56, 104
system safety engineer, 276
system testing, 273

T

TechnoDyne LLC, 42–43
technology
mobile, 314–315 (*See also* specific types of)
wireless, 314–315
Telecommunications Act, 184, 307
telecommuting, 304–305
telehealth, 315–317
telemedicine, 315–317
live, 316
store-and-forward, 315–316
telework, 304–305
Telework Improvement Act, 304
test/testing
black-box, 272
dynamic, 272
integration, 273
software, 272–273
static, 273
system, 273
user acceptance, 273
white-box, 272–273
Tetris, 223
text messaging, 94, 315
Third Circuit Court of Appeals, 195
ThisNext.com, 345
ThomasNet.com, 241
Thompson, Scott, 52
3M, 381
T.J. Maxx, 390
TJX, 390
Todd, Amanda, 191
Top-Level Domain names, 243
TopTenREVIEWS, 186
Toys “R” Us, 232

Trademark Act, 242
trademarks, 242
trade secrets, 46, 231–234
  definition of, 231, 232
  employees and, 233–234
  Federal Bureau of Investigation and, 233
  of Intel Corporation, 46
  laws for, 232–233
  misappropriation of, 231
  United States Patent and Trademark Office, protected by, 232
transaction-risk score, 98
transborder data flow, 147
TransUnion, 137
trap and trace order, 142–143
Treo, 238
TRIPS Agreement. *See* Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)
Trojan horses, 89–90
trustworthy computing
  activity logs, 111
  antivirus software, 107–108
  computer forensics, 112–114
  corporate firewall, 105–106
  cyberterrorism, 108–109
  definition of, 100
  detection, 110
  education on, 105
  eradication, 111
  evidence, 111
  implementation of, 100–114
  incident containment, 111
  incident follow-up, 111–112
  incident notification, 110
  Internet security threats, 109
  intrusion detection system, 106–107
  malicious insiders, 108
  by Microsoft, 100–101
  prevention and, 105–109
  response to, 110–114
  risk assessment and, 102–104
  security audits, 109
  security policy and, 104–105
Turnitin, 235–236
TUV NORD Group, 353
Twitter, 155
  Coca-Cola on, 342
  customer service and, 344
  cyberbullying on, 346
  defamation lawsuits, 184–185
  doxing on, 191
  hiring process and, 342
  inappropriate material on, 350
Tyco, 15

U

UFO incident at Roswell, 149
Uniform Commercial Code, 268
Uniform Domain Name Dispute Resolution Policy, 243
Union Army, 386
United Airlines, 65
UK Serious Fraud Office, 370
United Nations Convention Against Corruption, 51
United States Computer Emergency Readiness Team (US-CERT), 107
United States Patent and Trademark Office (USPTO), 228–230
  trademarks obtained from, 242
  trade secrets protected by, 232
USS *Vincennes*, 279
U.S. Army, 94
U.S. Bureau of Labor Statistics, 301, 304, 372, 374
U.S. Chamber of Commerce, 11
U.S. Citizenship and Immigration Services (USCIS), 377, 379–380
U.S. Code
  professional employee defined by, 44
  Title 15 of, 242
  Title 17 of, 222, 225
  Title 35 of, 229
U.S. Constitution, 134. *See also* specific amendments of
U.S. Department of Commerce, 148
U.S. Department of Defense, 7, 64–65, 94
U.S. Department of Education, 140
U.S. Department of Health and Human Services, 138–139
U.S. Department of Homeland Security (DHS), 11, 107–108, 151
U.S. Department of Justice, 370
  Adam Walsh Child Protection and Safety Act and, 350
  Education Rate program lawsuits by, 298
  electronic surveillance requests of, 141
  False Claims Act and, 386
  Foreign Corrupt Practices Act violations reported to, 65
  Office of the United States Intellectual Property Enforcement Representative within, 224
  social networking and, 343
U.S. Department of Labor (DOL), 376, 379–380
U.S. Federal Trade Commission (FTC), 12, 136, 140, 197

U.S. Food and Drug Administration, 156–157, 311
U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), 65
  healthcare and, 138–139
  requirements of, 138–139
  text messaging, 315
U.S. International Trade Commission, 219, 231
U.S. Navy, 191
U.S. Postal Service, 136
U.S. Securities and Exchange Commission (SEC), 6, 16, 65, 261, 370
U.S. stock markets, 262
U.S. Supreme Court
  First Amendment, interpretation by, 182, 184
  patents and, 229
  privacy, concept of, 134
  respondeat superior, principle of, 11
U.S. workers, H-1B workers *vs.*, 380
United States v. American Library Association, 188
United States v. Kilbride, 195
United States v. Little, 195
United States v. New York Central & Hudson River Railroad Co. (1909), 11
Universal Service Administrative Company (USAC), 297, 299–300, 307
University of California, Los Angeles, 351
University of Chicago, 307
University of Hong Kong, 52
University of Pittsburgh, 192
unreasonable government searches, 156
URL Internet filter/filtering, 185
Uruguay Round, 224
Uruguay Round Agreements Act, 224
USAC. *See* Universal Service Administrative Company (USAC)
USA Patriot (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act, 99, 142
US-CERT. *See* United States Computer Emergency Readiness Team (US-CERT)
USCIS. *See* U.S. Citizenship and Immigration Services (USCIS)
Usenet newsgroups, 192
user acceptance testing, 273
users
  expectations of, 86
  information technology, 61–66
USPTO. *See* United States Patent and Trademark Office (USPTO)
utilitarian approach, 23

V

VA. *See* Veterans Affairs (VA)
Valcich, Richard, 42
Vantiv, 234
vehicle event data recorders, 158–159
vendor certification, 57
Verizon, 192, 387
Vessel Hull Design Protection Act, 226
Veterans Affairs (VA), 151
VeteransNationalBank.us, 243
Viacom International, 227–228
viral marketing, 342
virtualization software, 86
virtual machines, 86
virtual private network (VPN), 105
virtual worlds
  online, 351–353
  Second Life, 341, 352
virtue, 4
virtue ethics approach, 23
viruses, 89
  ACAD/Medre.A, 97
  computer, 89
  definition of, 89
  macro, 89
  rootkit, 93
  true, 89
virus signature, 107
visa, 47
Visa Inc., 7, 98, 390
Visa Reform Act, 380
vishing, 94–95
Vision Systems Group, 380
Vizcaino v. Microsoft, 376–377
Voice over Internet Protocol (VoIP) technology, 143
VoIP. *See* Voice over Internet Protocol (VoIP) technology
VPN. *See* virtual private network (VPN)
vulnerability
  of commercial software, 87–88
  of Oracle Corporation software, 87

W

Wake Forest Baptist Medical Center, 314
Walsh, Adam, 350
Wanelo, 335–336, 344–345
warranty, 269–270
Washington State University, 265
Web anonymity, 191

Web sites
  medical information, 317–318
  social networking, 337–338, 342, 344–345
  social shopping, 335–336
Weiner, Anthony, 196, 350
Welles, Terri, 242
Wharton School of the University of Pennsylvania, 379
whistle-blowing, 47, 51, 385–390
  action plan for, 390
  consequences of, 390
  dealing with, 387–390
  definition of, 372
  documentation of, 388
  escalation within company, 388–389
  implications of, 389
  internally addressing, 388
  at Oracle Corporation, 387
  for private-sector workers, 387
  protection for, 386–387
  seriousness of, assessment of, 388
white-box testing, 272–273
Whitman, Meg, 370
WhoGotFunded.com, 241
Wigand, Jeffrey, 388
WikiLeaks, 62
Win-7 Anti-Virus 2012, 90
Windows, 83, 266, 309, 382
WIPO. *See* World Intellectual Property Organization (WIPO)
WIPO Copyright and Performances and Phonograms Treaties Implementation Act, 225–226
WIPO Performances and Phonograms Treaty, 225
wireless technology, 314–315
Wiretap Act, 141–143
wolfpacking, 351
Word, 93, 236
workers
  contingent, 374–377
  contract, 105
  H-1B, 377–381
  nontraditional, 372–373
  private-sector, 387
  US, 380
Working to Halt Online Abuse, 347
workplace
  environment, ethical, 18–19
  monitoring in, 155–157
  productivity in, standard of living and, 301–310
WorldCom, 15
World Intellectual Property Organization (WIPO), 225
World of Warcraft, 352
World Trade Organization (WTO), 224–225
worms, 89
  Blaster, 109
  Code Red, 89, 109
  Conficker, 89
  ILOVEYOU, 89
  Melissa, 89
  SirCam, 89
  Slammer, 109
  Storm, 89
WTO. *See* World Trade Organization (WTO)
Wyeth-Ayerst Laboratories, 10

X

Xavier University Preparatory School, 298
Xbox 360, 352
Xio Interactive, 223–224
XRDS, 55

Y

Yahoo!
  email service offered by, 90
  John Doe lawsuits against, 193
  résumé inflation at, 52
  telework programs of, 304
YouTube
  bullying on, 191
  Coca-Cola on, 342
  copyright infringement lawsuit against, 227–228
  creating account on, 194
  inappropriate material on, 350–351
  Internet filtering on, 186
  posting on, 194
  viral marketing on, 342

Z

Zappos, 152–153
Zenger, John, 190
zero-day attack, 88
zombies, 91
Zuckerberg, Mark, 48–49
Zynga, 47