جامعـــة الفيــوم
كلية الحاسبات والذكاء الاصطناعى
مؤسسة تعليمية معتمدة

الكتاب الجامعى
2023/2024

جامعة الفيوم

كلية الحاسبـــات
والذكاء الاصطناعى

أخلاقيات المهنة

Professional Ethics

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]

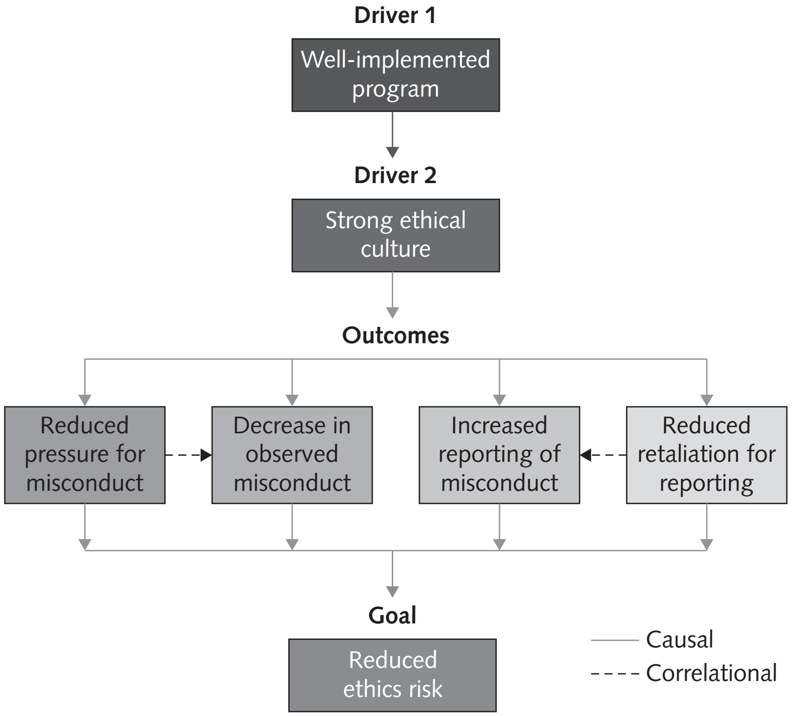

Driver 1
Well-implemented program
Driver 2
Strong ethical culture
Outcomes
Reduced pressure for misconduct
Decrease in observed misconduct
Increased reporting of misconduct
Reduced retaliation for reporting
Goal
Reduced ethics risk
Causal
Correlational

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

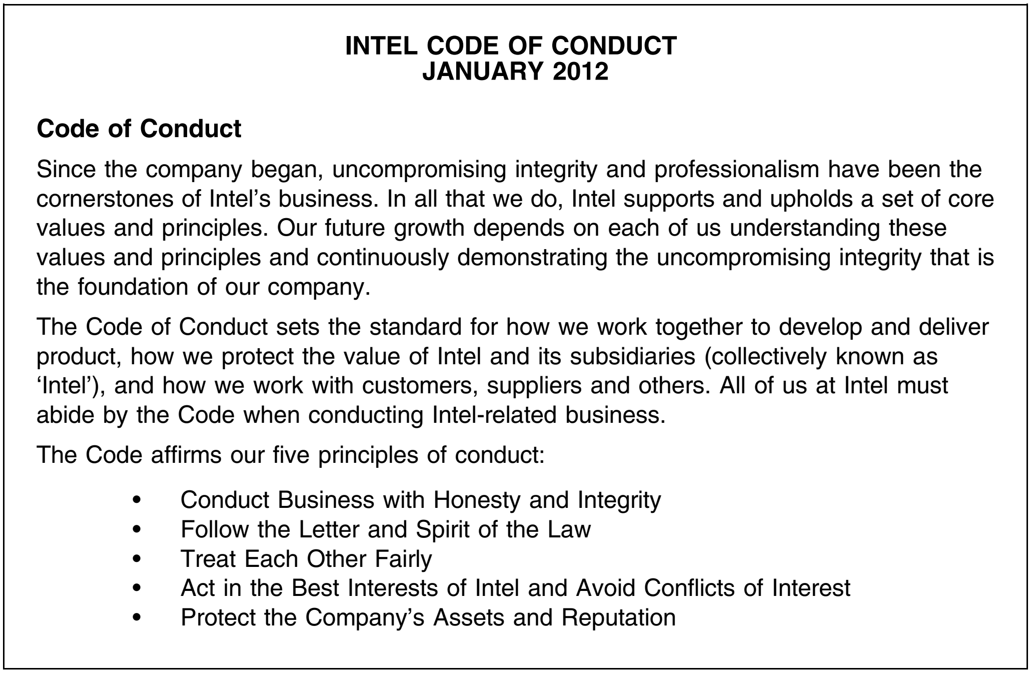
A **code of ethics** is a statement that highlights an organization's key ethical issues and identifies the overarching values and principles that are important to the organization and its decision making. Codes of ethics frequently include a set of formal, written statements about the purpose of an 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.

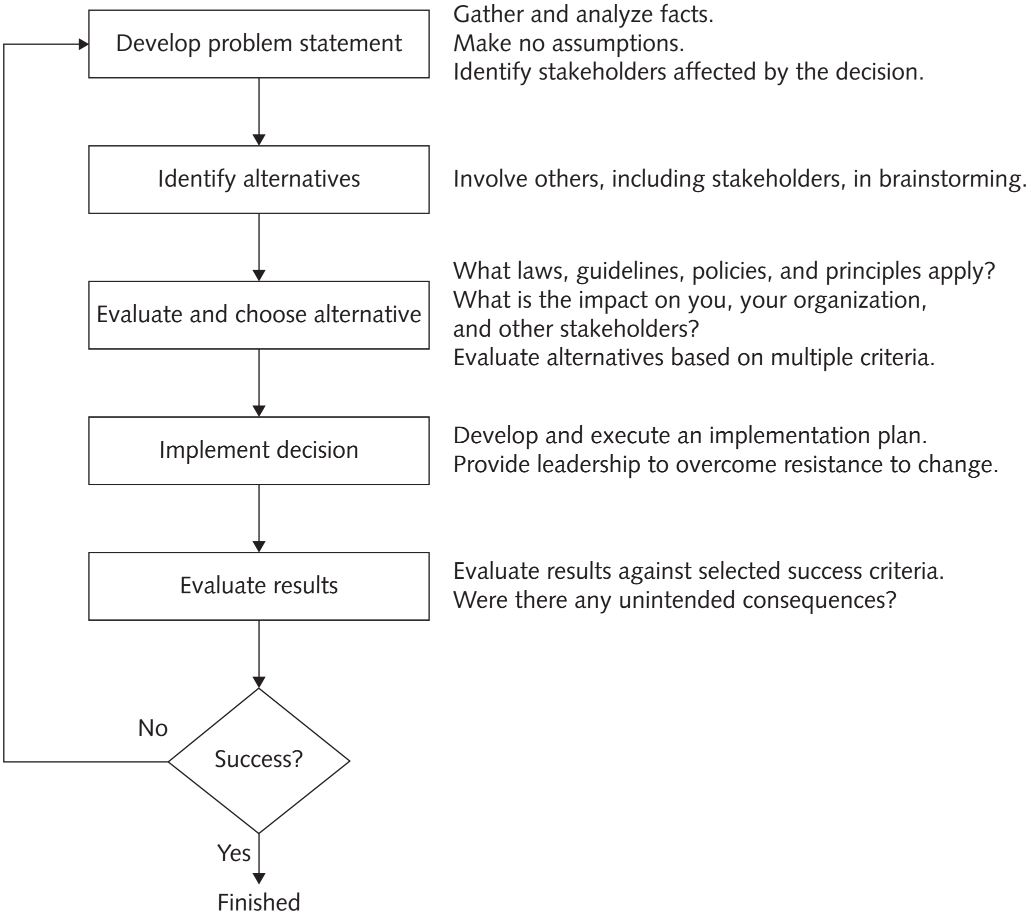

Develop problem statement
Gather and analyze facts.
Make no assumptions.
Identify stakeholders affected by the decision.
Identify alternatives
Involve others, including stakeholders, in brainstorming.
Evaluate and choose alternative
What laws, guidelines, policies, and principles apply?
What is the impact on you, your organization, and other stakeholders?
Evaluate alternatives based on multiple criteria.
Implement decision
Develop and execute an implementation plan.
Provide leadership to overcome resistance to change.
Evaluate results
Evaluate results against selected success criteria.
Were there any unintended consequences?
No
Success?
Yes
Finished

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.

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.

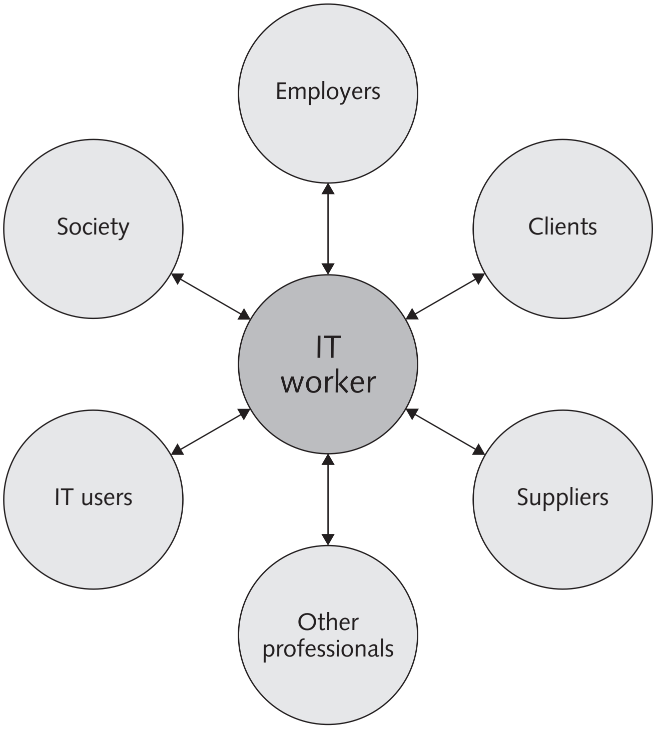


FIGURE 2-1 Professional relationships IT workers must manage
Credit: Course Technology/Cengage Learning.

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 whistle-blowers.[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 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:

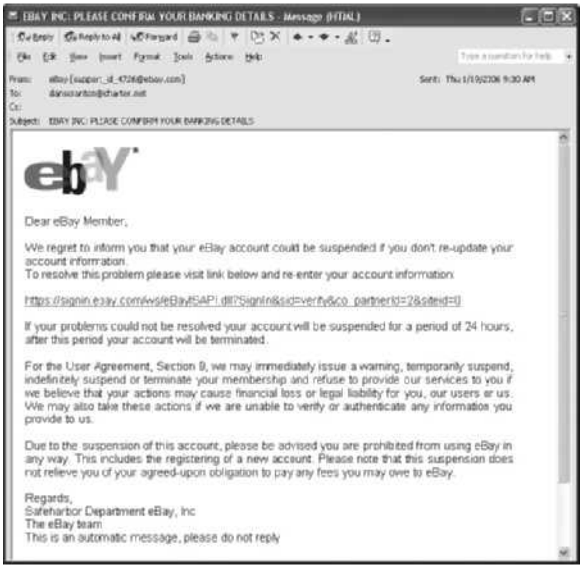
- The computer locks up or fails to respond to input from the keyboard or mouse.
- The screen saver changes without any action on the part of the user.
- The taskbar disappears.
- Network activities function extremely slowly.

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.



From: eBay [support_id_4726@ebay.com]
To: dansoranton@charter.net
Cc:
Subject: EBAY INC: PLEASE CONFIRM YOUR BANKING DETAILS
Sent: Thu 1/19/2006 9:30 AM

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

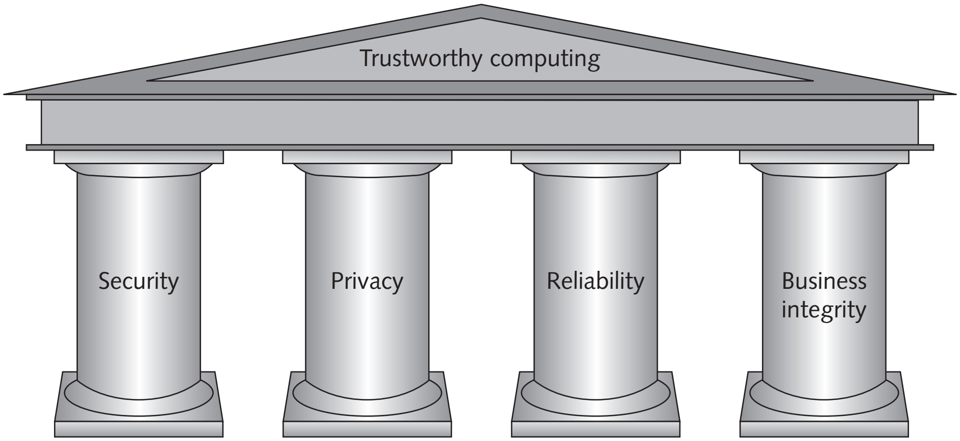


FIGURE 3-4 Microsoft's four pillars of trustworthy computing
Source Line: Course Technology/Cengage Learning.

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.

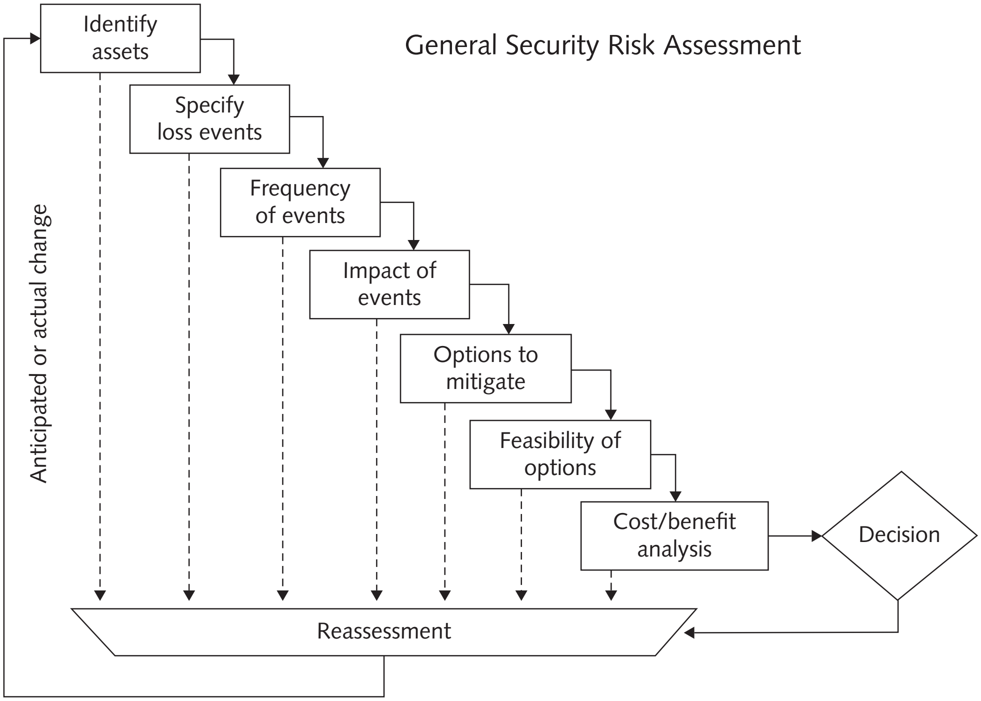


FIGURE 3-5 General security risk assessment

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.

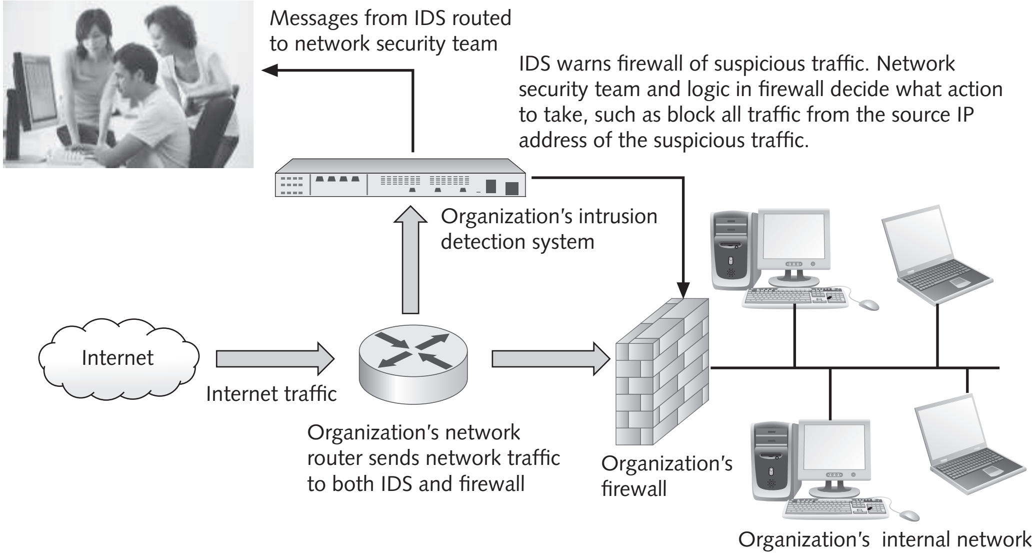

Messages from IDS routed to network security team
IDS warns firewall of suspicious traffic. Network security team and logic in firewall decide what action to take, such as block all traffic from the source IP address of the suspicious traffic.
Organization's intrusion detection system
Internet
Internet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

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 micromanaging 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]

Health Information

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

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