Ethics and Information Security: MIS Business Concerns

CHAPTER 4

CHAPTER OUTLINE

SECTION 4.1
Ethics

- Information Ethics
- Developing Information Management Policies
- Ethics in the Workplace

SECTION 4.2
Information Security

- Protecting Intellectual Assets
- The First Line of Defense—People
- The Second Line of Defense—Technology

What's in IT for me?

This chapter concerns itself with protecting information from potential misuse. Organizations must ensure they collect, capture, store, and use information in an ethical manner. This means any type of information they collect and utilize, including about customers, partners, and employees. Companies must ensure that personal information collected about someone remains private. This is not just a nice thing to do. The law requires it. Perhaps more important, information must be kept physically secure to prevent access and possible dissemination and use by unauthorized sources.

You, the business student, must understand ethics and security because they are the top concerns voiced by customers today. The way they are handled directly influences a customer's likelihood of embracing electronic technologies and conducting business over the Web–and thus the company's bottom line. You can find evidence in recent news reports about how the stock price of organizations falls dramatically when information privacy and security breaches are made known. Further, organizations face potential litigation if they fail to meet their ethical, privacy, and security obligations in the handling of information.

opening case study



E-Espionage

BusinessWeek magazine recently probed the rising attacks on America's most sensitive computer networks, uncovering startling security gaps. The email message addressed to a Booz Allen Hamilton executive from the Pentagon was mundane—a shopping list of weaponry India wanted to buy. But the missive was a brilliant fake. Lurking beneath the description of aircraft, engines, and radar equipment was an insidious piece of computer code, known as Poison Ivy, designed to suck sensitive data out of the $4 billion consulting firm's computer network.

The Pentagon had not sent the email. Its origin is unknown, but the message traveled through Korea on its way to Booz Allen. Its authors knew enough about the "sender" and "recipient" to craft a message unlikely to arouse suspicion. Had the Booz Allen executive clicked on the attachment, his every keystroke would have been reported back to a mysterious master at the Internet address cybersyndrome.3322.org, which is registered through an obscure company headquartered on the banks of China's Yangtze River.

The email aimed at Booz Allen paints a vivid picture of the alarming new capabilities of America's cyberenemies. The email message was sent to John F. "Jack" Mulhern, vice president for international military assistance programs at Booz Allen. In the high-tech world of weapons sales, Mulhern's specialty, the email looked authentic enough. "Integrate U.S., Russian, and Indian weapons and avionics," the email noted, describing the Indian government's expectations for its fighter jets. "Source code given to India for indigenous computer upgrade capability." Such lingo could easily be understood by Mulhern. The 62-year-old former U.S. Naval officer and 33-year veteran of Booz Allen's military consulting business is an expert in helping to sell U.S. weapons to foreign governments.

The email was more convincing because of its apparent sender: Stephen J. Moree, a civilian who works for a group that reports to the office of Air Force Secretary Michael W. Wynne. Among its duties, Moree's unit evaluates the security of selling U.S. military aircraft to other countries. There would be little reason to suspect anything seriously amiss in Moree passing along the highly technical document with "India MRCA Request for Proposal" in the subject line. The Indian government had just released the request a week earlier, on August 28, and the language in the email closely tracked the request. Making the message appear more credible still, it referred to upcoming Air Force communiqués and a "Team Meeting" to discuss the deal.

But the correspondence from Moree to Jack Mulhern was a fake. An analysis of the email's path and attachment, conducted for *BusinessWeek* by three cybersecurity specialists, shows it was sent by an unknown attacker, bounced through an Internet address in South Korea, relayed through a Yahoo! server in New York, and finally made its way to Mulhern's Booz Allen in-box. The analysis also shows the code—known as malware, for malicious software—tracks keystrokes on the computers of people who open it. A separate program disables security measures such as password protection on Microsoft Access database files, a program often used by large organizations such as the U.S. defense industry to manage big batches of data.

Global Threats

The U.S. government and its sprawl of defense contractors have been the victims of an unprecedented rash of similar attacks, say current and former U.S. government officials. "It's espionage on a massive scale," said Paul B. Kurtz, a former high-ranking national security official. Government agencies reported 12,986 cybersecurity incidents to the U.S. Homeland Security Department in one fiscal year, triple the number from two years earlier. Incursions on the military's networks were up 55 percent, said Lieutenant General Charles E. Croom, head of the Pentagon's Joint Task Force for Global Network Operations. Private targets such as Booz Allen are just as vulnerable and pose just as much potential security risk. "They have our information on their networks. They're building our weapon systems. You wouldn't want that in enemy hands," Croom said. Cyber attackers "are not denying, disrupting, or destroying operations—yet. But that doesn't mean they don't have the capability."

Poison Ivy

Commercial computer security firms have dubbed the malicious code hidden inside the email attachment Poison Ivy, and it has a devious—and worrisome—capability known as a RAT, a remote administration tool. RAT gives the attacker control over the host PC, capturing screen shots and perusing files. It lurks in the background of Microsoft Internet Explorer browsers while users surf the Web. Then it phones home to its "master" at an Internet address currently registered under the name cybersyndrome.3322.org.

The digital trail to cybersyndrome.3322.org, followed by analysts at *BusinessWeek*'s request, leads to one of China's largest free domain-name-registration and email services. Called 3322.org, it is registered to a company called Bentium in the city of Changzhou, an industrial hub outside Shanghai. A range of security experts say that 3322.org provides names for computers and servers that act as the command and control centers for more than 10,000 pieces of malicious code launched at government and corporate networks in recent years. Many of those PCs are in China; the rest could be anywhere.

The founder of 3322.org, a 37-year-old technology entrepreneur named Peng Yong, says his company merely allows users to register domain names. "As for what our users do, we cannot completely control it," Peng said. The bottom line: If Poison

Ivy infected Jack Mulhern's computer at Booz Allen, any secrets inside could be seen in China. And if it spread to other computers, as malware often does, the infection opens windows on potentially sensitive information there, too.

Many security experts worry the Internet has become too unwieldy to be tamed. New threats appear every day, each seemingly more sophisticated than the previous one. The Defense Department, whose Advanced Research Projects Agency (DARPA) developed the Internet in the 1960s, is beginning to think it created a monster. "You don't need an Army, a Navy, an Air Force to beat the U.S.," said General William T. Lord, commander of the Air Force Cyber Command, a unit formed to upgrade Air Force computer defenses. "You can be a peer force for the price of the PC on my desk."[1]

section 4.1 ETHICS

LEARNING OUTCOMES

4.1 Explain the ethical issues in the use of information technology.

4.2 Identify the six epolicies organizations should implement to protect themselves.

INFORMATION ETHICS

LO 4.1: Explain the ethical issues in the use of information technology.

Ethics and security are two fundamental building blocks for all organizations. In recent years, enormous business scandals along with 9/11 have shed new light on the meaning of ethics and security. When the behavior of a few individuals can destroy billion-dollar organizations, the value of ethics and security should be evident.

Copyright is the legal protection afforded an expression of an idea, such as a song, book, or video game. ***Intellectual property*** is intangible creative work that is embodied in physical form and includes copyrights, trademarks, and patents. As it becomes easier for people to copy everything from words and data to music and video, the ethical issues surrounding copyright infringement and the violation of intellectual property rights are consuming the ebusiness world. Technology poses new challenges for our ***ethics***—the principles and standards that guide our behavior toward other people.

The protection of customers' privacy is one of the largest, and murkiest, ethical issues facing organizations today. ***Privacy*** is the right to be left alone when you want to be, to have control over your personal possessions, and not to be observed without your consent. Privacy is related to ***confidentiality,*** which is the assurance that messages and information remain available only to those authorized to view them. Each time employees make a decision about a privacy issue, the outcome could sink the company.

Trust among companies, customers, partners, and suppliers is the support structure of ebusiness. Privacy is one of its main ingredients. Consumers' concerns that their privacy will be violated because of their interactions on the Web continue to be one of the primary barriers to the growth of ebusiness.

Information ethics govern the ethical and moral issues arising from the development and use of information technologies, as well as the creation, collection, duplication, distribution, and processing of information itself (with or without the aid of computer technologies). Ethical dilemmas in this area usually arise not as simple, clear-cut situations but as clashes among competing goals, responsibilities, and loyalties. Inevitably, there will be more than one socially acceptable or "correct" decision. The two primary areas concerning software include pirated software and counterfeit software. ***Pirated software*** is the unauthorized use, duplication, distribution, or sale of copyrighted software. ***Counterfeit software*** is software that is manufactured to look like the real thing and sold as such. Figure 4.1 contains examples of ethically questionable or unacceptable uses of information technology.[2]

Unfortunately, few hard and fast rules exist for always determining what is ethical. Many people can either justify or condemn the actions in Figure 4.1, for example. Knowing the law is important but that knowledge will not always help, because what is legal

Individuals copy, use, and distribute software.
Employees search organizational databases for sensitive corporate and personal information.
Organizations collect, buy, and use information without checking the validity or accuracy of the information.
Individuals create and spread viruses that cause trouble for those using and maintaining IT systems.
Individuals hack into computer systems to steal proprietary information.
Employees destroy or steal proprietary organization information such as schematics, sketches, customer lists, and reports.

FIGURE 4.1
Ethically Questionable or Unacceptable Information Technology Use

APPLY YOUR KNOWLEDGE

BUSINESS DRIVEN DISCUSSION

Information – Does It Have Ethics?

A high school principal decided it was a good idea to hold a confidential conversation about teachers, salaries, and student test scores on his cellular phone in a local Starbucks. Not realizing that one of the student's parents was sitting next to him, the principal accidentally divulged sensitive information about his employees and students. The irate parent soon notified the school board about the principal's inappropriate behavior and a committee was formed to decide how to handle the situation.[3]

With the new wave of collaboration tools, electronic business, and the Internet, employees are finding themselves working outside the office and beyond traditional office hours. Advantages associated with remote workers include increased productivity, decreased expenses, and boosts in morale as employees are given greater flexibility to choose their work location and hours. Unfortunately, there are also disadvantages associated with remote workers such as new forms of ethical challenges and information security risks.

In a group, discuss the following statement: Information Does Not Have Any Ethics. If you were elected to the committee to investigate the principal's inappropriate Starbucks phone conversation, what types of questions would you want answered? What type of punishment, if any, would you enforce on the principal? What types of policies would you implement across the school district to ensure this scenario is never repeated? Be sure to highlight how remote workers impact business along with any potential ethical challenges and information security issues.

might not always be ethical, and what might be ethical is not always legal. For example, Joe Reidenberg received an offer for AT&T cell phone service. AT&T used Equifax, a credit reporting agency, to identify potential customers such as Joe Reidenberg. Overall, this seemed like a good business opportunity between Equifax and AT&T wireless. Unfortunately, the Fair Credit Reporting Act (FCRA) forbids repurposing credit information except when the information is used for "a firm offer of credit or insurance." In other words, the only product that can be sold based on credit information is credit. A representative for Equifax stated, "As long as AT&T Wireless (or any company for that matter) is offering the cell phone service on a credit basis, such as allowing the use of the service before the consumer has to pay, it is in compliance with the FCRA." However, the question remains—is it ethical?[4]

This is a good example of the ethical dilemmas, many still being defined, that organizations face. Figure 4.2 shows the four quadrants of ethical and legal behavior. The goal for organizations is to make decisions within quadrant I that are *both* legal and ethical.

BUSINESS DRIVEN ETHICS AND SECURITY

Is IT Really Worth the Risk?

Ethics. It's just one tiny word, but it has monumental impact on every area of business. From the magazines, blogs, and newspapers you read to the courses you take, you will encounter ethics as it is a hot topic in today's electronic world. Technology has provided so many incredible opportunities, but it has also provided those same opportunities to unethical people. Discuss the ethical issues surrounding each of the following situations (yes, these are true stories):

- A student raises her hand in class and states, "I can legally copy any DVD I get from Netflix because Netflix purchased the DVD and the copyright only applies to the company who purchased the product."
- A student stands up the first day of class before the professor arrives and announces that his fraternity scans textbooks and he has the textbook for this course on his thumb drive, which he will gladly sell for $20. Several students pay on the spot and upload the scanned textbook to their PCs. One student takes down the student information and contacts the publisher about the incident.
- A senior marketing manager is asked to monitor his employee's email because there is a rumor that the employee is looking for another job.
- A vice president of sales asks her employee to burn all of the customer data onto an external hard drive because she made a deal to provide customer information to a strategic partner.
- A senior manager is asked to monitor his employee's email to discover if she is sexually harassing another employee.
- An employee is looking at the shared network drive and discovers his boss's entire hard drive, including his email backup, has been copied to the network and is visible to all.
- An employee is accidently copied on an email listing the targets for the next round of layoffs.

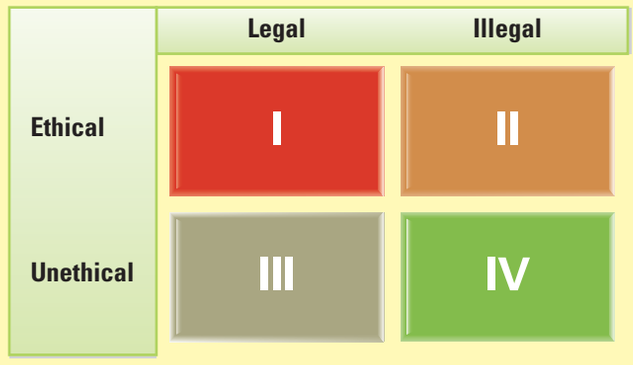


FIGURE 4.2
Acting Ethically and Acting Legally Are Not Always the Same

Information Does Not Have Ethics, People Do

Information itself has no ethics. It does not care how it is used. It will not stop itself from spamming customers, sharing itself if it is sensitive or personal, or revealing details to third parties. Information cannot delete or preserve itself. Therefore, it falls to those who own the information to develop ethical guidelines about how to manage it. ***Information management*** examines the organizational resource of information and regulates its definitions, uses, value, and distribution ensuring it has the types of data/information required to function and grow effectively. ***Information governance*** is a method or system of government for information management or control. ***Information***

FIGURE 4.3

Established Information-Related Laws

Established Information-Related Laws	
Privacy Act—1974	Restricts what information the federal government can collect; allows people to access and correct information on themselves; requires procedures to protect the security of personal information; and forbids the disclosure of name-linked information without permission.
Family Education Rights and Privacy Act—1974	Regulates access to personal education records by government agencies and other third parties and ensures the right of students to see their own records.
Cable Communications Act—1984	Requires written or electronic consent from viewers before cable TV providers can release viewing choices or other personally identifiable information.
Electronic Communications Privacy Act—1986	Allows the reading of communications by a firm and says that employees have no right to privacy when using their companies' computers.
Computer Fraud and Abuse Act—1986	Prohibits unauthorized access to computers used for financial institutions, the U.S. government, or interstate and international trade.
The Bork Bill (officially known as the Video Privacy Protection Act, 1988)	Prohibits the use of video rental information on customers for any purpose other than that of marketing goods and services directly to the customer.
Communications Assistance for Law Enforcement Act—1994	Requires that telecommunications equipment be designed so that authorized government agents are able to intercept all wired and wireless communications being sent or received by any subscriber. The act also requires that subscriber call-identifying information be transmitted to a government when and if required.
Freedom of Information Act—1967, 1975, 1994, and 1998	Allows any person to examine government records unless it would cause an invasion of privacy. It was amended in 1974 to apply to the FBI, and again in 1994 to allow citizens to monitor government activities and information gathering, and once again in 1998 to access government information on the Internet.
Health Insurance Portability and Accountability Act (HIPAA)—1996	Requires that the health care industry formulate and implement regulations to keep patient information confidential.
Identity Theft and Assumption Deterrence Act—1998	Strengthened the criminal laws governing identity theft making it a federal crime to use or transfer identification belonging to another. It also established a central federal service for victims.
USA Patriot Act—2001 and 2003	Allows law enforcement to get access to almost any information, including library records, video rentals, bookstore purchases, and business records when investigating any act of terrorist or clandestine intelligence activities. In 2003, Patriot II broadened the original law.
Homeland Security Act—2002	Provided new authority to government agencies to mine data on individuals and groups including emails and website visits; put limits on the information available under the Freedom of Information Act; and gave new powers to government agencies to declare national health emergencies.
Sarbanes-Oxley Act—2002	Sought to protect investors by improving the accuracy and reliability of corporate disclosures and requires companies to (1) implement extensive and detailed policies to prevent illegal activity within the company, and (2) to respond in a timely manner to investigate illegal activity.
Fair and Accurate Credit Transactions Act—2003	Included provisions for the prevention of identity theft including consumers' right to get a credit report free each year, requiring merchants to leave all but the last five digits of a credit card number off a receipt, and requiring lenders and credit agencies to take action even before a victim knows a crime has occurred when they notice any circumstances that might indicate identity theft.
CAN-Spam Act—2003	Sought to regulate interstate commerce by imposing limitations and penalties on businesses sending unsolicited email to consumers. The law forbids deceptive subject lines, headers, return addresses, etc., as well as the harvesting of email addresses from websites. It requires businesses that send spam to maintain a do-not-spam list and to include a postal mailing address in the message.

compliance is the act of conforming, acquiescing, or yielding information. A few years ago the ideas of information management, governance, and compliance were relatively obscure. Today, these concepts are a must for virtually every company, both domestic and global, primarily due to the role digital information plays in corporate legal proceedings or litigation. Frequently, digital information serves as key evidence in legal proceedings and it is far easier to search, organize, and filter than paper documents. Digital information is also extremely difficult to destroy especially if it is on a corporate network or sent via email. In fact, the only reliable way to truly obliterate digital information is to destroy the hard drives where the file was stored. ***Ediscovery*** (or ***electronic discovery***) refers to the ability of a company to identify, search, gather, seize, or export digital information in responding to a litigation, audit, investigation, or information inquiry. As the importance of ediscovery grows, so does information governance and information compliance. Figure 4.3 provides an overview of some of the important laws individuals and firms must follow in managing and protecting information.[5]

DEVELOPING INFORMATION MANAGEMENT POLICIES

LO 4.2: Identify the six epolicies organizations should implement to protect themselves.

Treating sensitive corporate information as a valuable resource is good management. Building a corporate culture based on ethical principles that employees can understand and implement is responsible management. Organizations should develop written policies establishing employee guidelines, employee procedures, and organizational rules for information. These policies set employee expectations about the organization's practices and standards and protect the organization from misuse of computer systems and IT resources. If an organization's employees use computers at work, the organization should, at a minimum, implement epolicies. ***Epolicies*** are policies and procedures that address information management along with the ethical use of computers and the Internet in the business environment. Figure 4.4 displays the epolicies a firm should implement to set employee expectations.

Ethical Computer Use Policy

In a case that illustrates the perils of online betting, a leading Internet poker site reported that a hacker exploited a security flaw to gain an insurmountable edge in high-stakes, no-limit Texas hold-'em tournaments—the ability to see his opponents' hole cards. The cheater, whose illegitimate winnings were estimated at between $400,000 and $700,000 by one victim, was an employee of AbsolutePoker.com and hacked the system to show that it could be done. Regardless of what business a company operates—even one that many view as unethical—the company must protect itself from unethical employee behavior.[6]

One essential step in creating an ethical corporate culture is establishing an ethical computer use policy. An ***ethical computer use policy*** contains general principles to guide computer user behavior. For example, it might explicitly state that users should refrain from playing computer games during working hours. This policy ensures the users know how to behave at work and the organization has a published standard to deal

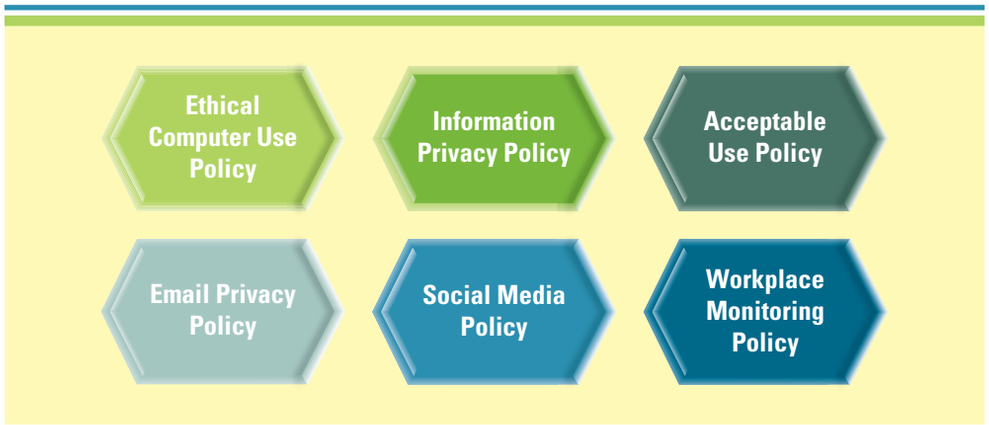


FIGURE 4.4
Overview of Epolicies

with infractions. For example, after appropriate warnings, the company may terminate an employee who spends significant amounts of time playing computer games at work.

Organizations can legitimately vary in how they expect employees to use computers, but in any approach to controlling such use, the overriding principle should be informed consent. The users should be *informed* of the rules and, by agreeing to use the system on that basis, *consent* to abide by them.

Managers should make a conscientious effort to ensure all users are aware of the policy through formal training and other means. If an organization were to have only one epolicy, it should be an ethical computer use policy because that is the starting point and the umbrella for any other policies the organization might establish.

Information Privacy Policy

An organization that wants to protect its information should develop an ***information privacy policy,*** which contains general principles regarding information privacy. Visa created Inovant to handle all its information systems including its coveted customer information, which details how people are spending their money, in which stores, on which days, and even at what time of day. Just imagine what a sales and marketing department could do if it gained access to this information. For this reason, Inovant bans the use of Visa's customer information for anything outside its intended purpose—billing. Innovant's privacy specialists developed a strict credit card information privacy policy, which it follows.

Now Inovant is being asked if it can guarantee that unethical use of credit card information will never occur. In a large majority of cases, the unethical use of information happens not through the malicious scheming of a rogue marketer, but rather unintentionally. For instance, information is collected and stored for some purpose, such as record keeping or billing. Then, a sales or marketing professional figures out another way to use it internally, share it with partners, or sell it to a trusted third party. The information is "unintentionally" used for new purposes. The classic example of this type of unintentional information reuse is the Social Security number, which started simply as a way to identify government retirement benefits and then was used as a sort of universal personal ID, found on everything from drivers' licenses to savings accounts.

Acceptable Use Policy

An ***acceptable use policy (AUP)*** requires a user to agree to follow it to be provided access to corporate email, information systems, and the Internet. ***Nonrepudiation*** is a contractual stipulation to ensure that ebusiness participants do not deny (repudiate) their online actions. A nonrepudiation clause is typically contained in an acceptable use policy. Many businesses and educational facilities require employees or students to sign an acceptable use policy before gaining network access. When signing up with an email provider, each customer is typically presented with an AUP, which states the user agrees to adhere to certain stipulations. Users agree to the following in a typical acceptable use policy:

- Not using the service as part of violating any law.
- Not attempting to break the security of any computer network or user.
- Not posting commercial messages to groups without prior permission.
- Not performing any nonrepudiation.

Some organizations go so far as to create a unique information management policy focusing solely on Internet use. An ***Internet use policy*** contains general principles to guide the proper use of the Internet. Because of the large amounts of computing resources that Internet users can expend, it is essential that such use be legitimate. In addition, the Internet contains numerous materials that some believe are offensive, making regulation in the workplace a requirement. Generally, an Internet use policy:

- Describes the Internet services available to users.
- Defines the organization's position on the purpose of Internet access and what restrictions, if any, are placed on that access.

BUSINESS DRIVEN GLOBALIZATION

Censoring Google

The Google debate over operations in China is an excellent example of types of global ethical and security issues U.S. companies face as they expand operations around the world. Google's systems were targeted by highly sophisticated hacker attacks aimed at obtaining proprietary information including personal data belonging to Chinese human rights activists who use Google's Gmail service. Google, which originally agreed to filter search results based on Chinese government censorship rules, decided to unfilter search results after what it called an infiltration of its technology and the email accounts of Chinese human-rights activists. China called Google's plan to defy government censorship rules unfriendly and irresponsible and demanded Google shut down all operations in China.

Why would China want to filer search results? Do you agree or disagree with China's censorship rules? Do you think Google was acting ethically when it agreed to implement China's censorship rules? Why do companies operating abroad need to be aware of the different ethical perspective found in other cultures?[7]

- Describes user responsibility for citing sources, properly handling offensive material, and protecting the organization's good name.
- States the ramifications if the policy is violated.

Email Privacy Policy

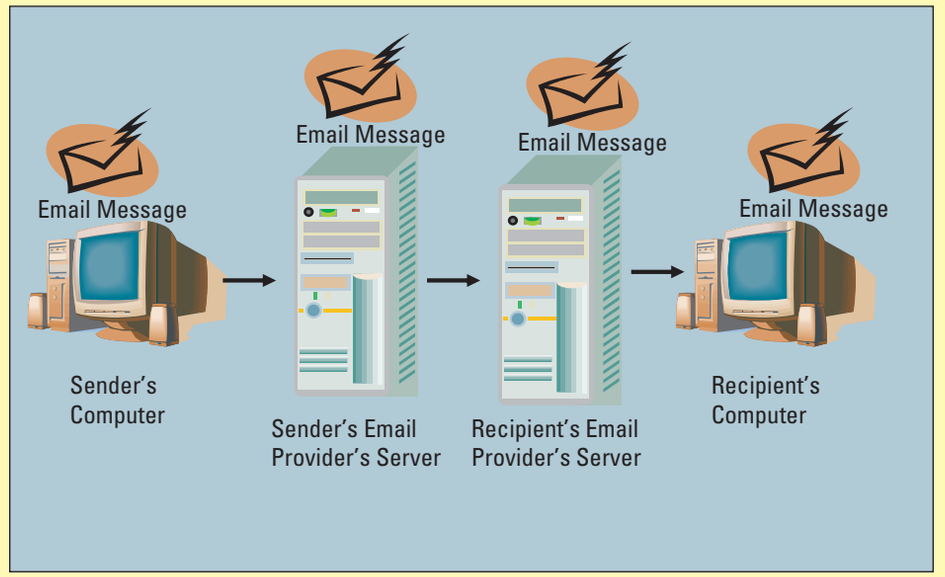
An ***email privacy policy*** details the extent to which email messages may be read by others. Email is so pervasive in organizations that it requires its own specific policy. Most working professionals use email as their preferred means of corporate communications. While email and instant messaging are common business communication tools, there are risks associated with using them. For instance, a sent email is stored on at least three or four computers (see Figure 4.5). Simply deleting an email from one computer does not delete it from the others. Companies can mitigate many of the risks of using electronic messaging systems by implementing and adhering to an email privacy policy.

One major problem with email is the user's expectations of privacy. To a large extent, this expectation is based on the false assumption that email privacy protection exists somehow analogous to that of U.S. first-class mail. Generally, the organization that owns the email system can operate the system as openly or as privately as it wishes. Surveys indicate that the majority of large firms regularly read and analyze employees' email looking for confidential data leaks such as unannounced financial results or the sharing of trade secrets that result in the violation of an email privacy policy and eventual termination of the employee. That means that if the organization wants to read everyone's email, it can do so. Basically, using work email for anything other than work is not a good idea. A typical email privacy policy:

- Defines legitimate email users and explains what happens to accounts after a person leaves the organization.
- Explains backup procedure so users will know that at some point, even if a message is deleted from their computer, it is still stored by the company.
- Describes the legitimate grounds for reading email and the process required before such action is performed.
- Discourages sending junk email or spam to anyone who does not want to receive it.

FIGURE 4.5

Email Is Stored on Multiple Computers



- Prohibits attempting to mail bomb a site. A ***mail bomb*** sends a massive amount of email to a specific person or system that can cause that user's server to stop functioning.
- Informs users that the organization has no control over email once it has been transmitted outside the organization.

Spam is unsolicited email. It plagues employees at all levels within an organization, from receptionist to CEO, and clogs email systems and siphons MIS resources away from legitimate business projects. An ***anti-spam policy*** simply states that email users will not send unsolicited emails (or spam). It is difficult to write anti-spam policies, laws, or software because there is no such thing as a universal litmus test for spam. One person's spam is another person's newsletter. End users have to decide what spam is, because it can vary widely not just from one company to the next, but from one person to the next.

Social Media Policy

Did you see the YouTube video showing two Domino's Pizza employees violating health codes while preparing food by passing gas on sandwiches? Millions of people did and the company took notice when disgusted customers began posting negative comments all over Twitter. Not having a Twitter account, corporate executives at Domino's did not know about the damaging tweets until it was too late. The use of social media can contribute many benefits to an organization, and implemented correctly it can become a huge opportunity for employees to build brands. But there are also tremendous risks as a few employees representing an entire company can cause tremendous brand damage. Defining a set of guidelines implemented in a social media policy can help mitigate that risk. Companies can protect themselves by implementing a ***social media policy*** outlining the corporate guidelines or principles governing employee online communications. Having a single social media policy might not be enough to ensure the company's online reputation is protected. Additional, more specific, social media policies a company might choose to implement include:[8]

- Employee online communication policy detailing brand communication.
- Employee blog and personal blog policies.
- Employee social network and personal social network policies.

BUSINESS DRIVEN MIS

Sources Are Not Friends

The Canadian Broadcasting Company (CBC) has issued a social networking policy directing journalists to avoid adding sources or contacts as friends on social networking sites such as Facebook or LinkedIn. Basic rules state that reporters never allow one source to view what another source says and reporters want to ensure private conversations with sources remain private. Adding sources as "friends" can compromise a journalist's work by allowing friends to view other friends in the network. It may also not be in a journalist's best interest to become a "friend" in a source's network. The CBC also discourages posting any political preferences in personal profiles, commenting on bulletin boards or people's "Facebook wall."

This might seem like common sense, but for employees who do not spend countless hours on the Internet, using social networking sites can be confusing and overwhelming. Why is it critical for any new hire to research and review all policies, especially social media policies? Research three companies you would like to work for upon graduation, and detail the types of social media policies that the company currently has or should implement.[9]

- Employee Twitter, corporate Twitter, and personal Twitter policies.
- Employee LinkedIn policy.
- Employee Facebook usage and brand usage policy.
- Corporate YouTube policy.

Organizations must protect their online reputations and continuously monitor blogs, message boards, social networking sites, and media sharing sites. However, monitoring the hundreds of different social media sites can quickly become overwhelming. To combat these issues, a number of companies specialize in online social media monitoring; for example, Trackur.com creates digital dashboards allowing executives to view at a glance the date published, source, title, and summary of every item tracked. The dashboard not only highlights what's being said, but also the influence of the particular person, blog, or social media site.

Workplace Monitoring Policy

Increasingly, employee monitoring is not a choice; it is a risk-management obligation. Michael Soden, CEO of the Bank of Ireland, issued a mandate stating that company employees could not surf illicit websites with company equipment. Next, he hired Hewlett-Packard to run the MIS department and illicit websites were discovered on Soden's own computer, forcing Soden to resign. Monitoring employees is one of the biggest challenges CIOs face when developing information management policies.[10]

New technologies make it possible for employers to monitor many aspects of their employees' jobs, especially on telephones, computer terminals, through electronic and voice mail, and when employees are using the Internet. Such monitoring is virtually unregulated. Therefore, unless company policy specifically states otherwise (and even this is not assured), your employer may listen, watch, and read most of your workplace communications. ***Information technology monitoring*** tracks people's activities by such measures as number of keystrokes, error rate, and number of transactions processed (see Figure 4.6 for an overview). The best path for an organization planning to engage in employee monitoring is open communication including an ***employee monitoring policy*** stating explicitly how, when, and where the company monitors its employees.

FIGURE 4.6
Internet Monitoring Technologies

Common Internet Monitoring Technologies	
Key logger, or key trapper, software	A program that records every keystroke and mouse click.
Hardware key logger	A hardware device that captures keystrokes on their journey from the keyboard to the motherboard.
Cookie	A small file deposited on a hard drive by a website containing information about customers and their web activities. Cookies allow websites to record the comings and goings of customers, usually without their knowledge or consent.
Adware	Software that generates ads that install themselves on a computer when a person downloads some other program from the Internet.
Spyware (sneakware or stealthware)	Software that comes hidden in free downloadable software and tracks online movements, mines the information stored on a computer, or uses a computer's CPU and storage for some task the user knows nothing about.
Web log	Consists of one line of information for every visitor to a website and is usually stored on a web server.
Clickstream	Records information about a customer during a Web surfing session such as what websites were visited, how long the visit was, what ads were viewed, and what was purchased.

Several common stipulations an organization can follow when creating an employee monitoring policy include:

- Be as specific as possible stating when and what (email, IM, Internet, network activity, etc.) will be monitored.
- Expressly communicate that the company reserves the right to monitor all employees.
- State the consequences of violating the policy.
- Always enforce the policy the same for everyone.

Many employees use their company's high-speed Internet access to shop, browse, and surf the Web. Most managers do not want their employees conducting personal business during working hours, and they implement a Big Brother approach to employee monitoring. Many management gurus advocate that organizations whose corporate cultures are based on trust are more successful than those whose corporate cultures are based on mistrust. Before an organization implements monitoring technology, it should ask itself, "What does this say about how we feel about our employees?" If the organization really does not trust its employees, then perhaps it should find new ones. If an organization does trust its employees, then it might want to treat them accordingly. An organization that follows its employees' every keystroke might be unwittingly undermining the relationships with its employees, and it might find the effects of employee monitoring are often worse than lost productivity from employee Web surfing.

section 4.2 INFORMATION SECURITY

LEARNING OUTCOMES

4.3 Describe the relationships and differences between hackers and viruses.

4.4 Describe the relationship between information security policies and an information security plan.

4.5 Provide an example of each of the three primary information security areas: (1) authentication and authorization, (2) prevention and resistance, and (3) detection and response.

BUSINESS DRIVEN DEBATE

Fired for Smoking on the Weekend

New technologies make it possible for employers to monitor many aspects of their employees' jobs, especially on telephones, computer terminals, through electronic and voice mail, and when employees are using the Internet. Such monitoring is virtually unregulated. Therefore, unless company policy specifically states otherwise (and even this is not assured), your employer may listen, watch, and read most of your workplace communications.

Employers are taking monitoring activity a step further and monitoring employees, and employees' spouses, at home and on weekends. Yes, you read that correctly. Numerous employees have been fired for smoking cigarettes on the weekend in the privacy of their own home. As health care costs escalate, employers are increasingly seeking to regulate employee behavior—at home as well as in the workplace. Weyco, an insurance benefits administrator in Michigan, initiated a program requiring mandatory breath tests to detect for nicotine, and any employee testing positive would be sent home without pay for one month. If the employee failed the nicotine test a second time, that person would be fired—no matter how long the employee had been with the company. Weyco's smoking prohibition does not stop with employees but extends to spouses also who must pass monthly nicotine tests. A positive test means the employee must pay a monthly fee of $80 until the spouse takes a smoking-cessation program and tests nicotine-free.[11]

Do you agree that companies have the right to hold employees accountable for actions they perform on weekends in the privacy of their own homes? If you were the CEO of Weyco, what would be your argument supporting its smoking prohibition policies? Do you think Weyco's monitoring practices are ethical? Do you think Weyco's monitoring practices are legal?

PROTECTING INTELLECTUAL ASSETS

LO 4.3: Describe the relationships and differences between hackers and viruses.

To accurately reflect the crucial interdependence between MIS and business processes, we should update the old business axiom "Time is money" to say "Uptime is money." ***Downtime*** refers to a period of time when a system is unavailable. Unplanned downtime can strike at any time for any number of reasons, from tornadoes to sink overflows to network failures to power outages (see Figure 4.7). Although natural disasters may appear to be the most devastating causes of MIS outages, they are hardly the most frequent or most expensive. Figure 4.8 demonstrates that the costs of downtime are not only associated with lost revenues, but also with financial performance, damage to reputations, and even travel or legal expenses. A few questions managers should ask when determining the cost of downtime are:[12]

- How many transactions can the company afford to lose without significantly harming business?
- Does the company depend upon one or more mission-critical applications to conduct business?
- How much revenue will the company lose for every hour a critical application is unavailable?
- What is the productivity cost associated with each hour of downtime?
- How will collaborative business processes with partners, suppliers, and customers be affected by an unexpected IT outage?
- What is the total cost of lost productivity and lost revenue during unplanned downtime?

FIGURE 4.7

Sources of Unplanned Downtime

Sources of Unplanned Downtime		
Bomb threat	Frozen pipe	Snowstorm
Burst pipe	Hacker	Sprinkler malfunction
Chemical spill	Hail	Static electricity
Construction	Hurricane	Strike
Corrupted data	Ice storm	Terrorism
Earthquake	Insects	Theft
Electrical short	Lightning	Tornado
Epidemic	Network failure	Train derailment
Equipment failure	Plane crash	Smoke damage
Evacuation	Power outage	Vandalism
Explosion	Power surge	Vehicle crash
Fire	Rodents	Virus
Flood	Sabotage	Water damage (various)
Fraud	Shredded data	Wind

FIGURE 4.8

The Cost of Downtime

The reliability and resilience of IT systems have never been more essential for success as businesses cope with the forces of globalization, 24/7 operations, government and trade regulations, global recession, and overextended IT budgets and resources. Any unexpected downtime in today's business environment has the potential to cause both short- and long-term costs with far-reaching consequences.

Information security is a broad term encompassing the protection of information from accidental or intentional misuse by persons inside or outside an organization. Information security is the primary tool an organization can use to combat the threats associated with downtime. Understanding how to secure information systems is critical to keeping downtime to a minimum and uptime to a maximum. Hackers and viruses are two of the hottest issues currently facing information security.

Security Threats Caused by Hackers and Viruses

Hackers are experts in technology who use their knowledge to break into computers and computer networks, either for profit or just motivated by the challenge. Smoking is not just bad for a person's health; it seems it is also bad for company security as hackers regularly use smoking entrances to gain building access. Once inside they pose as employees from the MIS department and either ask for permission to use an employee's computer to access the corporate network, or find a conference room where they simply plug-in their own laptop. Figure 4.9 lists the various types of hackers organizations need to be aware of, and Figure 4.10 shows how a virus is spread.

FIGURE 4.9
Types of Hackers

Common Types of Hackers
■ ***Black-hat hackers*** break into other people's computer systems and may just look around or may steal and destroy information.
■ ***Crackers*** have criminal intent when hacking.
■ ***Cyberterrorists*** seek to cause harm to people or to destroy critical systems or information and use the Internet as a weapon of mass destruction.
■ ***Hactivists*** have philosophical and political reasons for breaking into systems and will often deface the website as a protest.
■ ***Script kiddies*** or ***script bunnies*** find hacking code on the Internet and click-and-point their way into systems to cause damage or spread viruses.
■ ***White-hat hackers*** work at the request of the system owners to find system vulnerabilities and plug the holes.

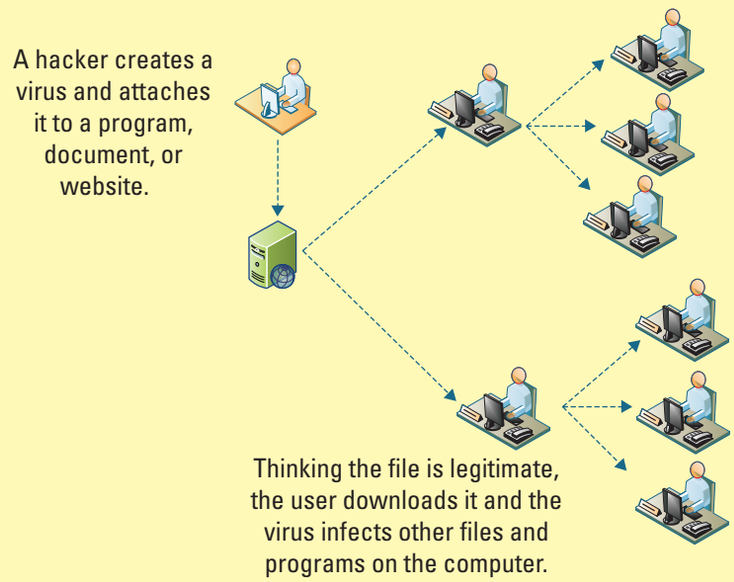


FIGURE 4.10
How Computer Viruses Spread

One of the most common forms of computer vulnerabilities is a virus. A ***virus*** is software written with malicious intent to cause annoyance or damage. Some hackers create and leave viruses causing massive computer damage. Figure 4.11 provides an overview of the most common types of viruses. Two additional computer vulnerabilities include adware and spyware. ***Adware*** is software that, while purporting to serve some useful function and often fulfilling that function, also allows Internet advertisers to display advertisements without the consent of the computer user. ***Spyware*** is a special class of adware that collects data about the user and transmits it over the Internet without the user's knowledge or permission. Spyware programs collect specific data about the user, ranging from general demographics such as name, address, and browsing habits to credit card numbers, Social Security numbers, and user names and passwords. Not all adware programs are spyware and used correctly it can generate revenue for a company allowing users to receive free products. Spyware is a clear threat to privacy. Figure 4.12 displays a few additional weapons hackers use for launching attacks.[13]

Organizational information is intellectual capital. Just as organizations protect their tangible assets—keeping their money in an insured bank or providing a safe working environment for employees—they must also protect their intellectual capital, everything

FIGURE 4.11

Common Forms of Viruses

Backdoor programs open a way into the network for future attacks.
Denial-of-service attack (DoS) floods a website with so many requests for service that it slows down or crashes the site.
Distributed denial-of-service attack (DDoS) attacks from multiple computers that flood a website with so many requests for service that it slows down or crashes. A common type is the Ping of Death, in which thousands of computers try to access a website at the same time, overloading it and shutting it down.
Polymorphic viruses and worms change their form as they propagate.
Trojan-horse virus hides inside other software, usually as an attachment or a downloadable file.
Worm spreads itself, not only from file to file, but also from computer to computer. The primary difference between a virus and a worm is that a virus must attach to something, such as an executable file, to spread. Worms do not need to attach to anything to spread and can tunnel themselves into computers.

FIGURE 4.12

Hacker Weapons

Elevation of privilege is a process by which a user misleads a system into granting unauthorized rights, usually for the purpose of compromising or destroying the system. For example, an attacker might log onto a network by using a guest account and then exploit a weakness in the software that lets the attacker change the guest privileges to administrative privileges.
Hoaxes attack computer systems by transmitting a virus hoax, with a real virus attached. By masking the attack in a seemingly legitimate message, unsuspecting users more readily distribute the message and send the attack on to their co-workers and friends, infecting many users along the way.
Malicious code includes a variety of threats such as viruses, worms, and Trojan horses.
Packet tampering consists of altering the contents of packets as they travel over the Internet or altering data on computer disks after penetrating a network. For example, an attacker might place a tap on a network line to intercept packets as they leave the computer. The attacker could eavesdrop or alter the information as it leaves the network.
A **sniffer** is a program or device that can monitor data traveling over a network. Sniffers can show all the data being transmitted over a network, including passwords and sensitive information. Sniffers tend to be a favorite weapon in the hacker's arsenal.
Spoofing is the forging of the return address on an email so that the message appears to come from someone other than the actual sender. This is not a virus but rather a way by which virus authors conceal their identities as they send out viruses.
Splogs (spam blogs) are fake blogs created solely to raise the search engine rank of affiliated websites. Even blogs that are legitimate are plagued by spam, with spammers taking advantage of the Comment feature of most blogs to comments with links to spam sites.
Spyware is software that comes hidden in free downloadable software and tracks online movements, mines the information stored on a computer, or uses a computer's CPU and storage for some task the user knows nothing about.

from patents to transactional and analytical information. With security breaches and viruses on the rise and computer hackers everywhere, an organization must put in place strong security measures to survive.

THE FIRST LINE OF DEFENSE—PEOPLE

LO 4.4: Describe the relationship between information security policies and an information security plan.

Organizations today are able to mine valuable information such as the identity of the top 20 percent of their customers, who usually produce 80 percent of revenues. Most organizations view this type of information as intellectual capital and implement security measures to prevent it from walking out the door or falling into the wrong hands. At the same time, they must enable employees, customers, and partners to access needed information electronically. Organizations address security risks through two lines of defense; the first is people, the second technology.

Surprisingly, the biggest problem is people as the majority of information security breaches result from people misusing organizational information. ***Insiders*** are legitimate users who purposely or accidentally misuse their access to the environment and cause some kind of business-affecting incident. For example, many individuals freely give up their passwords or write them on sticky notes next to their computers, leaving the door wide open for hackers. Through ***social engineering,*** hackers use their social skills to trick people into revealing access credentials or other valuable information. ***Dumpster diving,*** or looking through people's trash, is another way hackers obtain information.

Information security policies identify the rules required to maintain information security, such as requiring users to log off before leaving for lunch or meetings, never sharing passwords with anyone, and changing passwords every 30 days. An ***information security plan*** details how an organization will implement the information security policies. The best way a company can safeguard itself from people is by implementing and communicating its information security plan. This becomes even more important with Web 2.0 and as the use of mobile devices, remote workforce, and contractors are growing. A few details managers should consider surrounding people and information security policies include defining the best practices for[14]

- Applications allowed to be placed on the corporate network, especially various file sharing applications (Kazaz), IM software, and entertainment or freeware created by unknown sources (iPhone applications).
- Corporate computer equipment used for personal reason on personal networks.
- Password creation and maintenance including minimum password length, characters to be included while choosing passwords, and frequency for password changes.
- Personal computer equipment allowed to connect to the corporate network.
- Virus protection including how often the system should be scanned and how frequently the software should be updated. This could also include if downloading attachments is allowed and practices for safe downloading from trusted and untrustworthy sources.

THE SECOND LINE OF DEFENSE—TECHNOLOGY

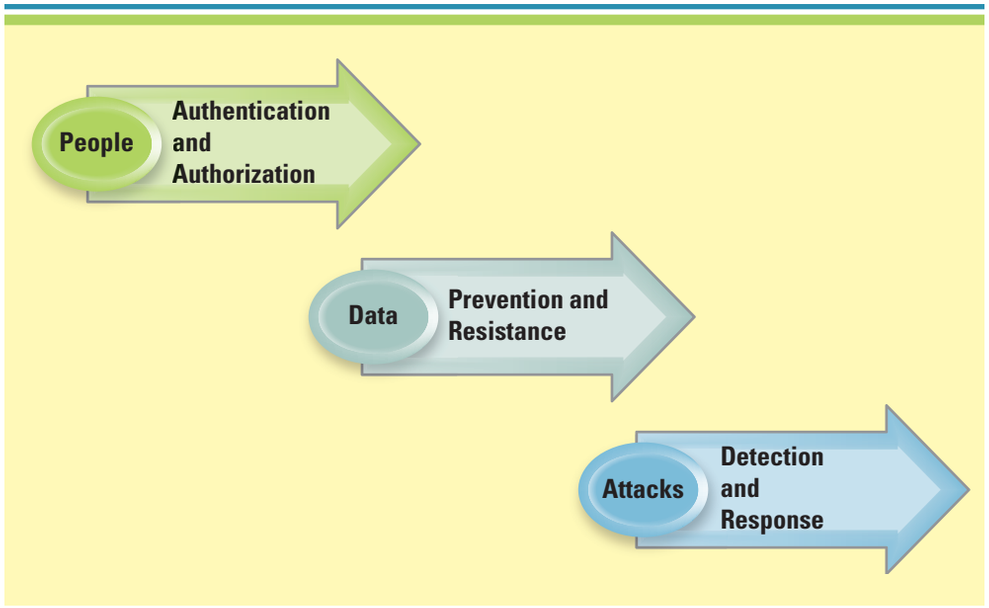
LO 4.5: Provide an example of each of the three primary information security areas: (1) authentication and authorization, (2) prevention and resistance, and (3) detection and response.

Once an organization has protected its intellectual capital by arming its people with a detailed information security plan, it can begin to focus on deploying technology to help combat attackers. Figure 4.13 displays the three areas where technology can aid in the defense against attacks.

People: Authentication and Authorization

Identity theft is the forging of someone's identity for the purpose of fraud. The fraud is often financial, because thieves apply for and use credit cards or loans in the victim's name. Two means of stealing an identity are phishing and pharming. ***Phishing*** is a technique to gain personal information for the purpose of identity theft, usually by means of fraudulent emails that look as though they came from legitimate businesses. The messages appear to be genuine, with official-looking formats and logos, and typically

FIGURE 4.13
Three Areas of Information Security



ask for verification of important information such as passwords and account numbers, ostensibly for accounting or auditing purposes. Since the emails look authentic, up to one in five recipients responds with the information and subsequently becomes a victim of identity theft and other fraud. Figure 4.14 displays a phishing scam attempting to gain information for Bank of America; you should never click on emails asking you to verify your identity as companies will never contact you directly asking for your user name or password.[15]

Pharming reroutes requests for legitimate websites to false websites. For example, if you were to type in the URL to your bank, pharming could redirect to a fake site that collects your information. Authentication and authorization technologies can prevent identity theft, phishing, and pharming scams. ***Authentication*** is a method for confirming users' identities. Once a system determines the authentication of a user, it can then determine the access privileges (or authorization) for that user. ***Authorization*** is the process of providing a user with permission including access levels and abilities such as file access, hours of access, and amount of allocated storage space. Authentication and authorization techniques fall into three categories; the most secure procedures combine all three:

1. Something the user knows, such as a user ID and password.
2. Something the user has, such as a smart card or token.
3. Something that is part of the user, such as a fingerprint or voice signature.

Something the User Knows Such as a User ID and Password The first type of authentication, using something the user knows, is the most common way to identify individual users and typically consists of a unique user ID and password. However, this is actually one of the most *ineffective* ways for determining authentication because passwords are not secure. All it typically takes to crack one is enough time. More than 50 percent of help-desk calls are password related, which can cost an organization significant money, and a social engineer can coax a password from almost anybody.

Something the User Has Such as a Smart Card or Token The second type of authentication, using something the user has, offers a much more effective way to identify individuals than a user ID and password. Tokens and smart cards are two of the primary forms of this type of authentication. ***Tokens*** are small electronic devices that change user passwords automatically. The user enters his or her user ID and token-displayed password to gain access to the network. A ***smart card*** is a device about the size of a credit card, containing embedded technologies that can store information and

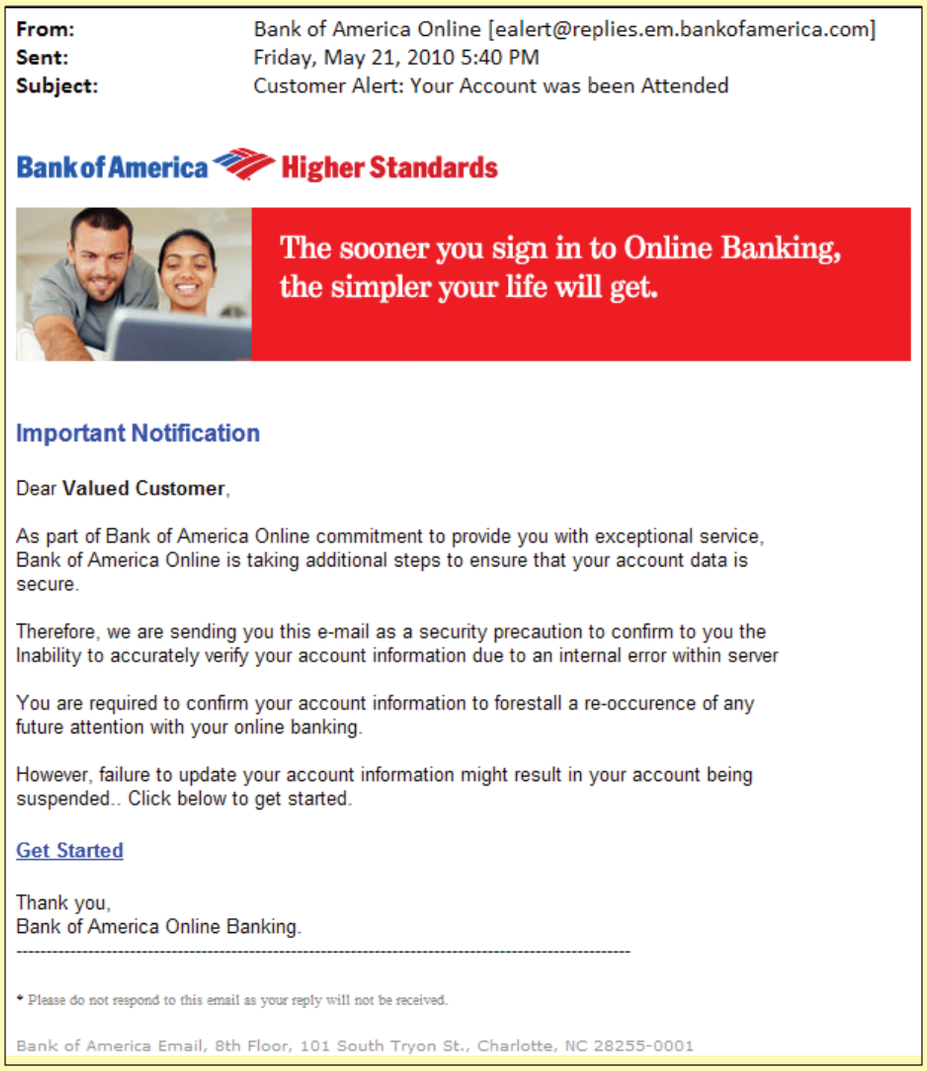


FIGURE 4.14
Bank of America Phishing Scam

small amounts of software to perform some limited processing. Smart cards can act as identification instruments, a form of digital cash, or a data storage device with the ability to store an entire medical record.

Something That Is Part of the User Such as a Fingerprint or Voice Signature The third kind of authentication, something that is part of the user, is by far the best and most effective way to manage authentication. ***Biometrics*** (narrowly defined) is the identification of a user based on a physical characteristic, such as a fingerprint, iris, face, voice, or handwriting. Unfortunately, biometric authentication can be costly and intrusive.

Data: Prevention and Resistance

Prevention and resistance technologies stop intruders from accessing and reading data by means of content filtering, encryption, and firewalls. ***Content filtering*** occurs when organizations use software that filters content, such as emails, to prevent the accidental or malicious transmission of unauthorized information. Organizations can use content filtering technologies to filter email and prevent emails containing sensitive information from transmitting, whether the transmission was malicious or accidental. It can also filter emails and prevent any suspicious files from transmitting such as potential virus-infected files. Email content filtering can also filter for spam, a form of unsolicited email.

APPLY YOUR KNOWLEDGE

BUSINESS DRIVEN INNOVATION

Doodling Passwords

As our online world continues to explode, people are finding the number of user names and passwords they need to remember growing exponentially. For this reason many users will assign the same password for every log-on, choose easy to remember names and dates, or simply write down their passwords on sticky notes and attach them to their computers. Great for the person who needs to remember 72 different passwords, but not so great for system security.

Of course the obvious answer is to deploy biometrics across the board, but once you start reviewing the costs associated with biometrics you quickly realize that this is not feasible. What is coming to the rescue to help with the password nightmare we have created? The doodle. Background Draw-a-Secret (BDAS) is a new program created by scientists at Newcastle University in England. BDAS begins by recording the number of strokes it takes a user to draw a doodle and when the user wants to gain access to the system he simply redraws the doodle on a touchpad and it is matched against the stored prototype. If the doodle matches, the user is granted access. Doodles are even described as being far more anonymous, therefore offering great security, than biometrics.

You are probably thinking that you'll end up right back in the same position having to remember all 72 of your password doodles. The good news is that with doodle passwords you don't have to remember a thing. The doodle password can be displayed to users, and they simply have to redraw it since the system analyzes how the user draws or the user's unique hand strokes, not the actual doodle (similar to handwriting recognition technologies).[16]

If you were going to deploy doodle passwords to your organization, what issues and concerns do you think might occur? Do you agree that doodles are easier to remember than text passwords? Do you agree that doodles offer the most effective way to manage authentication and authorization, even greater than biometrics? What types of unethical issues do you think you might encounter with doodle passwords?

Encryption scrambles information into an alternative form that requires a key or password to decrypt. If there were a security breach and the stolen information were encrypted, the thief would be unable to read it. Encryption can switch the order of characters, replace characters with other characters, insert or remove characters, or use a mathematical formula to convert the information into a code. Companies that transmit sensitive customer information over the Internet, such as credit card numbers, frequently use encryption.

Some encryption technologies use multiple keys. ***Public key encryption (PKE)*** uses two keys: a public key that everyone can have and a private key for only the recipient (see Figure 4.15). The organization provides the public key to all customers, whether end consumers or other businesses, who use that key to encrypt their information and send it via the Internet. When it arrives at its destination, the organization uses the private key to unscramble it.

Public keys are becoming popular to use for authentication techniques consisting of digital objects in which a trusted third party confirms correlation between the user and the public key. A ***certificate authority*** is a trusted third party, such as VeriSign, that validates user identities by means of digital certificates. A ***digital certificate*** is a data file that identifies individuals or organizations online and is comparable to a digital signature.

A ***firewall*** is hardware and/or software that guard a private network by analyzing incoming and outgoing information for the correct markings. If they are missing, the

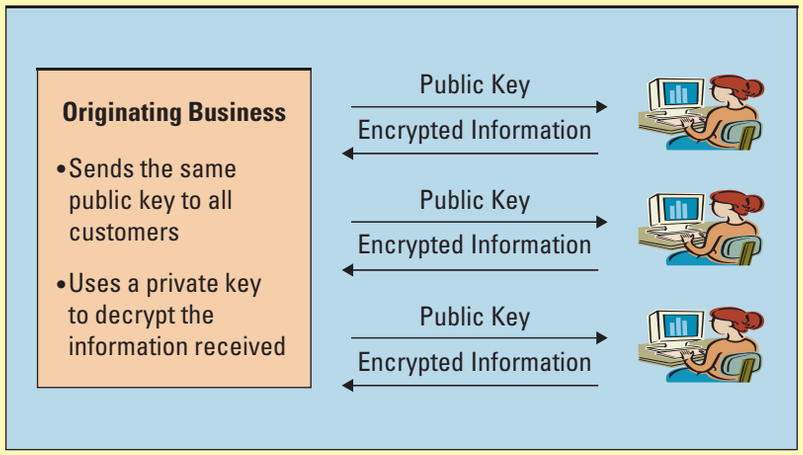


FIGURE 4.15
Public Key Encryption (PKE)

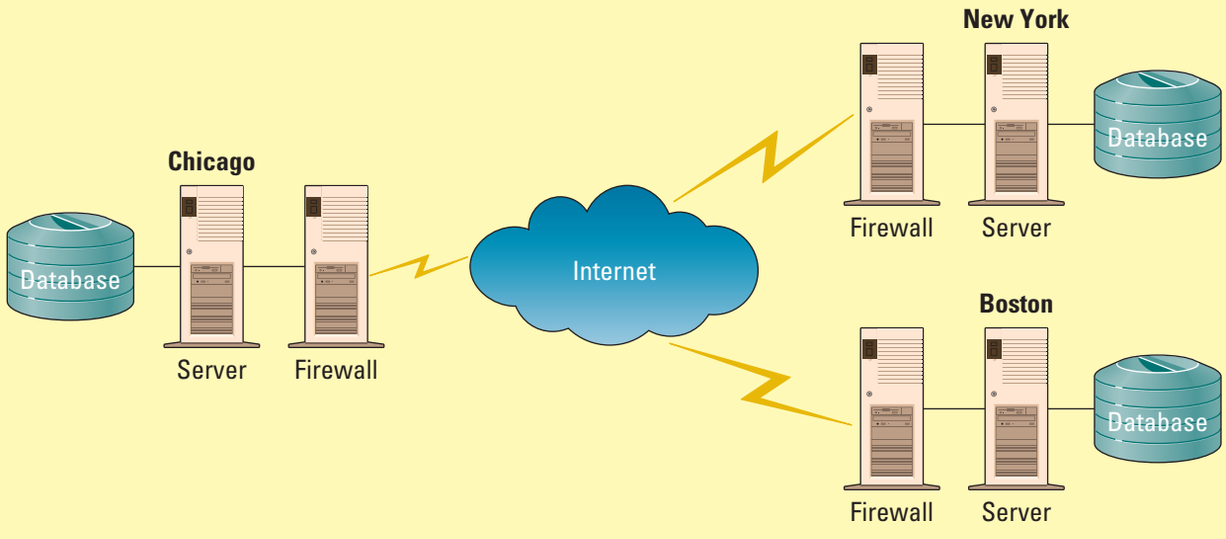
firewall prevents the information from entering the network. Firewalls can even detect computers communicating with the Internet without approval. As Figure 4.16 illustrates, organizations typically place a firewall between a server and the Internet. Think of a firewall as a gatekeeper that protects computer networks from intrusion by providing a filter and safe transfer points for access to and from the Internet and other networks. It screens all network traffic for proper passwords or other security codes and allows only authorized transmissions in and out of the network.

Firewalls do not guarantee complete protection, and users should enlist additional security technologies such as antivirus software and antispyware software. ***Antivirus software*** scans and searches hard drives to prevent, detect, and remove known viruses, adware, and spyware. Antivirus software must be frequently updated to protect against newly created viruses.

Attack: Detection and Response

The presence of an intruder can be detected by watching for suspicious network events such as bad passwords, the removal of highly classified data files, or unauthorized user attempts. ***Intrusion detection software (IDS)*** features full-time monitoring tools that search for patterns in network traffic to identify intruders. IDS protects against suspicious

FIGURE 4.16
Sample Firewall Architecture Connecting Systems Located in Chicago, New York, and Boston



APPLY YOUR KNOWLEDGE

BUSINESS DRIVEN START-UP

LifeLock: Keeping Your Identity Safe

Have you ever seen a LifeLock advertisement? If so, you know the Social Security number of LifeLock CEO Todd Davis because he posts it in all ads daring hackers to try to steal his identity. Davis has been a victim of identity theft at least 13 times. The first theft occurred when someone used his identity to secure a $500 loan from a check-cashing company. Davis discovered the crime only after the company called his wife's cell phone to recover the unpaid debt.[17]

If you were starting an identity theft prevention company, do you think it would be a good idea to post your Social Security number in advertisements? Why or why not? What do you think happened that caused Davis' identity to be stolen? What types of information security measure should LifeLock implement to ensure Davis' Social Security number is not stolen again? If you were LifeLock's CEO, what type of marketing campaign would you launch next?

network traffic and attempts to access files and data. If a suspicious event or unauthorized traffic is identified, the IDS will generate an alarm and can even be customized to shut down a particularly sensitive part of a network. After identifying an attack, an MIS department can implement response tactics to mitigate the damage. Response tactics outline procedures such as how long a system under attack will remain plugged in and connected to the corporate network, when to shut down a compromised system, and how quickly a backup system will be up and running.

Guaranteeing the safety of organization information is achieved by implementing the two lines of defense: people and technology. To protect information through people, firms should develop information security policies and plans that provide employees with specific precautions they should take in creating, working with, and transmitting the organization's information assets. Technology-based lines of defense fall into three categories: authentication and authorization; prevention and resistance; and detection and response.

LEARNING OUTCOME REVIEW

Learning Outcome 4.1: Explain the ethical issues in the use of information technology.

Information ethics govern the ethical and moral issues arising from the development and use of information technologies, as well as the creation, collection, duplication, distribution, and processing of information itself (with or without the aid of computer technologies). Ethical dilemmas in this area usually arise not as simple, clear-cut situations but as clashes between competing goals, responsibilities, and loyalties. Inevitably, there will be more than one socially acceptable or "correct" decision. For this reason, acting ethically and legally are not always the same.

Learning Outcome 4.2: Identify the six epolicies organizations should implement to protect themselves.

1. An ethical computer use policy contains general principles to guide computer user behavior. For example, it might explicitly state that users should refrain from playing computer games during working hours.

2. An information privacy policy contains general principles regarding information privacy.
3. An acceptable use policy (AUP) is a policy that a user must agree to follow in order to be provided access to corporate email, information systems, and to the Internet.
4. An email privacy policy details the extent to which email messages may be read by others.
5. A social media policy outlines the corporate guidelines or principles governing employee online communications.
6. An employee monitoring policy states explicitly how, when, and where the company monitors its employees.

Learning Outcome 4.3: Describe the relationships and differences between hackers and viruses.

Hackers are experts in technology who use their knowledge to break into computers and computer networks, either for profit or just motivated by the challenge. A virus is software written with malicious intent to cause annoyance or damage. Some hackers create and leave viruses causing massive computer damage.

Learning Outcome 4.4: Describe the relationship between information security policies and an information security plan.

Information security policies identify the rules required to maintain information security, such as requiring users to log off before leaving for lunch or meetings, never sharing passwords with anyone, and changing passwords every 30 days. An information security plan details how an organization will implement the information security policies. The best way a company can safeguard itself from people is by implementing and communicating its information security plan.

Learning Outcome 4.5: Provide an example of each of the three primary information security areas: (1) authentication and authorization, (2) prevention and resistance, and (3) detection and response.

Authentication and authorization: Authentication is a method for confirming users' identities. Once a system determines the authentication of a user, it can then determine the access privileges (or authorization) for that user. Authorization is the process of providing a user with permission including access levels and abilities such as file access, hours of access, and amount of allocated storage space.

Prevention and resistance: Content filtering occurs when organizations use software that filters content, such as emails, to prevent the accidental or malicious transmission of unauthorized information. Encryption scrambles information into an alternative form that requires a key or password to decrypt. In a security breach, a thief is unable to read encrypted information. A firewall is hardware and/or software that guard a private network by analyzing incoming and outgoing information for the correct markings.

Detection and response: Intrusion detection software (IDS) features full-time monitoring tools that search for patterns in network traffic to identify intruders.

OPENING CASE QUESTIONS

1. **Knowledge:** Define information ethics and information security and explain why each are critical to any government operation.
2. **Comprehension:** Identify two epolicies the government should implement to help combat cyberterrorism.

3. **Application:** Demonstrate how the government can use authentication and authorization technologies to prevent information theft.
4. **Analysis:** Analyze how the government can use prevention and resistance technologies to safeguard its employees from hackers and viruses.
5. **Synthesis:** Propose a plan for how the government can implement information security plans to ensure its critical information is safe and protects.
6. **Evaluate:** Evaluate the information security issues facing the government and identify its three biggest concerns.

KEY TERMS

Acceptable use policy (AUP), 140
Adware, 148
Anti-spam policy, 142
Antivirus software, 153
Authentication, 150
Authorization, 150
Biometrics, 151
Black-hat hackers, 147
Certificate authority, 152
Confidentiality, 135
Content filtering, 151
Copyright, 135
Counterfeit software, 135
Cracker, 147
Cyberterrorists, 147
Digital certificate, 152
Downtime, 145
Dumpster diving, 149
Ediscovery (or electronic discovery), 139
Email privacy policy, 141
Employee monitoring policy, 143
Encryption, 152
Epolicies, 139
Ethical computer use policy, 139
Ethics, 135
Firewall, 152
Hackers, 147
Hactivists, 147
Identity theft, 149
Information compliance, 138–139
Information ethics, 135
Information governance, 138
Information management, 138
Information privacy policy, 140
Information security, 147
Information security plan, 149
Information security policies, 149
Information technology monitoring, 143
Insiders, 149
Intellectual property, 135
Internet use policy, 140
Intrusion detection software (IDS), 153
Mail bomb, 142
Nonrepudiation, 140
Pharming, 150
Phishing, 149
Pirated software, 135
Privacy, 135
Public key encryption (PKE), 152
Script kiddies or script bunnies, 147
Smart card, 150
Social engineering, 149
Social media policy, 142
Spam, 142
Spyware, 148
Tokens, 150
Virus, 148
White-hat hackers, 147

REVIEW QUESTIONS

1. What are ethics and why are they important to a company?
2. What is the relationship between information management, governance, and compliance?
3. Why are epolicies important to a company?
4. What is the correlation between privacy and confidentiality?
5. What is the relationship between adware and spyware?
6. What are the positive and negative effects associated with monitoring employees?
7. What is the relationship between hackers and viruses?
8. Why is security a business issue, not just a technology issue?
9. What are the growing issues related to employee communication methods and what can a company do to protect itself?
10. How can a company participating in ebusiness keep its information secure?
11. What technologies can a company use to safeguard information?

12. Why is ediscovery important to a company?
13. What are the reasons a company experiences downtime?
14. What are the costs associated with downtime?

CLOSING CASE ONE

Banks Banking on Security

Bank of America, Commerce Bancorp, PNC Financial Services Group, and Wachovia were victims of a crime where a person tried to steal customer data and sell it to law firms and debt-collection agencies. The thief was selling 670,000 account numbers and balances to the undercover New Jersey police. Increasing network security is a key factor for banks as this is a deciding factor when customers compare financial institutions.

Bank of America

Bank of America is moving toward a stronger authentication process using SiteKey. A service designed to spoil scams in which customers think they are entering data on the bank's website but are actually on a thief's website that is stealing customer data. Worms tell the computers to reroute the URL for the bank into a different site that looks exactly like the banks cite. With SiteKey, a customer can select an image and associate a brief written passage. Whenever the customer signs onto the website, they will see their selected image along with the passage ensuring they are on the bank's website. If the customer is using a different computer the website will ask additional identification questions.

Wells Fargo & Company

"Out-of-wallet" questions contain information not found on identification cards in a wallet such as a driver's license or ATM card. Wells Fargo is implementing a security strategy that operates based on "out-of-wallet" questions for passwords.

E-Trade Financial Corporation

E-Trade Financial Corporation provides customers who have account balances exceeding $50,000 a free Digital Security ID for network authentication. The device displays a new six-digit code every 60 seconds, which the customer must use to log on. Accounts under $50,000 can purchase the Digital Security ID device for $25.

Barclays Bank

Barclays Bank delays money transfers between several hours and one day allowing the company the ability to detect suspicious activity, such as a large number of transfers from multiple accounts into a single account. The online-transfer delay keeps transfers safe from mules, or people who open bank accounts based on an email solicitation. Thieves withdraw cash or open credit cards from the mule accounts.[18]

Questions

1. What reason would a bank have for not wanting to adopt an online-transfer delay policy?
2. What are the two primary lines of security defense and why are they important to financial institutions?
3. Explain the differences between the types of security offered by the banks in the case. Which bank would you open an account with and why?

4. What additional types of security, not mentioned in the case, would you recommend a bank implement?
5. Identify three epolicies a bank should implement to help it improve information security.
6. Describe monitoring policies along with the best way for a bank to implement monitoring technologies.

CLOSING CASE TWO

Hacker Hunters

Hacker hunters are the new breed of crime fighter. They employ the same methodology used to fight organized crime in the 1980s—informants and the cyberworld equivalent of wiretaps. Daniel Larking, a 20-year veteran who runs the FBI's Internet Crime Complaint Center, taps online service providers to help track down criminal hackers. Leads supplied by the FBI and eBay helped Romanian police round up 11 members of a gang that set up fake eBay accounts and auctioned off cell phones, laptops, and cameras they never intended to deliver.

The FBI unleashed Operation Firewall, targeting the ShadowCrew, a gang whose members were schooled in identity theft, bank account pillage, and selling illegal goods on the Internet. ShadowCrew's 4,000 gang members lived in a dozen countries and across the United States. For months, agents had been watching their every move through a clandestine gateway into their website, shadowcrew.com. One member turned informant and called a group meeting, ensuring the members would be at home on their computers during a certain time, when the Secret Service issued orders to move in on the gang. The move was synchronized around the globe to prevent gang members from warning each other via instant messages. Twenty-eight gang members in eight states and six countries were arrested, most still at their computers. Authorities seized dozens of computers and found 1.7 million credit card numbers and more than 18 million email accounts.

ShadowCrew's Operations

The alleged ringleaders of ShadowCrew included Andres Mantovani, 23, a part-time community college student in Arizona, and David Appleyard, 45, a former New Jersey mortgage broker. Mantovani and Appleyard allegedly were administrators in charge of running the website and recruiting members. The site created a marketplace for more than 4,000 gang members who bought and sold hot information and merchandise. The website was open for business 24 hours a day, but since most of the members held jobs, the busiest time was from 10 p.m. to 2 a.m. on Sundays. Hundreds of gang members would meet online to trade credit card information, passports, and even equipment to make fake identity documents. Platinum credit cards cost more than gold ones, and discounts were offered for package deals. One member known as "Scarface" sold 115,695 stolen credit card numbers in a single trade. Overall, the gang made more than $4 million in credit card purchases over two years. ShadowCrew was equivalent to an eBay for the underworld. The site even posted crime tips on how to use stolen credit cards and fake IDs at big retailers.

The gang stole credit card numbers and other valuable information through clever tricks. One of the favorites was sending millions of phishing emails—messages that appeared to be from legitimate companies such as Yahoo!—designed to steal passwords and credit card numbers. The gang also hacked into corporate databases to steal account data. According to sources familiar with the investigation, the gang cracked the networks of 12 unidentified companies that were not even aware their systems had been breached.

Police Operations

Brian Nagel, an assistant director at the Secret Service, coordinated the effort to track the ShadowCrew. Allies included Britain's national high-tech crimes unit, the Royal Canadian Mounted Police, and the Bulgarian Interior Ministry. Authorities turned one of the high-ranking members of the gang into a snitch and had the man help the Secret Service set up a new electronic doorway for ShadowCrew members to enter their website. The snitch spread the word that the new gateway was a more secure way to the website. It was the first-ever tap of a private computer network. "We became shadowcrew.com," Nagel said. Mantovani and Appleyard were slated for trial. Authorities anticipated making additional arrests.[19]

Questions

1. What types of technology could big retailers use to prevent identity thieves from purchasing merchandise?
2. What can organizations do to protect themselves from hackers looking to steal account data?
3. Authorities frequently tap online service providers to track down hackers. Do you think it is ethical for authorities to tap an online service provider and read people's email? Why or why not?
4. Do you think it was ethical for authorities to use one of the high-ranking officials to trap other gang members? Why or why not?
5. In a team, research the Internet and find the best ways to protect yourself from identity theft.

CRITICAL BUSINESS THINKING

1. Cheerleader Charged $27,750 for File Sharing 37 Songs

A federal appeals court is ordering a university student to pay the Recording Industry Association of America $27,750—$750 a track—for file sharing 37 songs when she was a high school cheerleader. Have you ever illegally copied or downloaded a song or movie? If you have and you were forced to pay $750 per track, how much would you owe? What is the difference between file sharing and Internet radio streaming? Do you agree or disagree with the federal appeals decision? Why or why not? Why is claiming a lack of copyright knowledge not a good defense against illegally sharing movies or music? If you do not have a good understanding of information laws, what can you do to ensure you are never placed in a federal lawsuit for violating information laws?[20]

2. Police Records Found in Old Copy Machine

Copy machines made after 2002 all contain a hard drive that stores a copy of every document the machine has ever scanned, printed, copied, or faxed. If the hard drive is not erased or scrubbed when the copy machine is resold, all of that digital information is still maintained inside the machine. The Buffalo, New York, Police Sex Crimes Division recently sold several copy machines without scrubbing the hard drives. The hard drives yielded detailed domestic violence complaints and a list of wanted sex offenders. A machine from the Buffalo Police Narcotics Unit contained targets in a major drug raid, and a copier once used by a New York construction company stored 95 pages of pay stubs with names, addresses, and Social Security numbers.[21]

Who do you think should be held responsible for the information issues caused at the Buffalo police department? What types of ethical issues and information security issues

are being violated? What types of epolicies could a company implement to ensure these situations do not occur? What forms of information security could a company implement to ensure these situations do not occur? How does this case support the primary reason why ediscovery is so important to litigation?

3. Firewall Decisions

You are the CEO of Inverness Investments, a medium-size venture capital firm that specializes in investing in high-tech companies. The company receives more than 30,000 email messages per year. On average, there are two viruses and three successful hackings against the company each year, which result in losses to the company of about $250,000. Currently, the company has antivirus software installed but does not have any firewalls.

Your CIO is suggesting implementing 10 firewalls for a total cost of $80,000. The estimated life of each firewall is about three years. The chances of hackers breaking into the system with the firewalls installed are about 3 percent. Annual maintenance costs on the firewalls are estimated around $15,000. Create an argument for or against supporting your CIO's recommendation to purchase the firewalls. Are there any considerations in addition to finances?

4. Preventing Identity Theft

The FBI states that identity theft is one of the fastest-growing crimes. If you are a victim of identity theft, your financial reputation can be ruined, making it impossible for you to cash a check or receive a bank loan. Learning how to avoid identity theft can be a valuable activity. Research the following websites and draft a document stating the best ways to prevent identity theft.

- The Federal Trade Commission Consumer Information on ID theft at www.consumer.gov/idtheft.
- The Office of the Comptroller of the Currency at www.occ.treas.gov/chcktfd.idassume.htm.
- The Office of the Inspector General at www.ssa.gov/oig/when.htm.
- U.S. Department of Justice at www.usdoj.gov/criminal/fraud/idtheft.html.

5. Discussing the Three Areas of Information Security

Great Granola Inc. is a small business operating out of northern California. The company specializes in selling homemade granola, and its primary sales vehicle is through its website. The company is growing exponentially and expects its revenues to triple this year to $12 million. The company also expects to hire 60 additional employees to support its growth. Joan Martin, the CEO, is aware that if her competitors discover the recipe for her granola, or who her primary customers are, it could easily ruin her business. Martin has hired you to draft a document discussing the different areas of information security, along with your recommendations for providing a secure ebusiness environment.

6. Spying on Email

Technology advances now allow individuals to monitor computers that they do not even have physical access to. New types of software can capture an individual's incoming and outgoing email and then immediately forward that email to another person. For example, if you are at work and your child is home from school and she receives an email from John at 3:00 p.m., at 3:01 p.m. you can receive a copy of that email sent to your email address. If she replies to John's email, within seconds you will again receive a copy of what she sent to John. Describe two scenarios (other than those described here) for the use of this type of software: one in which the use would be ethical and one in which it would be unethical.

7. Stealing Software

The software industry fights against pirated software on a daily basis. The major centers of software piracy are in places such as Russia and China where salaries and disposable income are comparatively low. People in developing and economically depressed countries will fall behind the industrialized world technologically if they cannot afford access to new generations of software. Considering this, is it reasonable to blame someone for using pirated software when it could cost him or her two months' salary to purchase a legal copy? Create an argument for or against the following statement: Individuals who are economically less fortunate should be allowed access to software free of charge in order to ensure that they are provided with an equal technological advantage.

ENTREPRENEURIAL CHALLENGE

BUILD YOUR OWN BUSINESS

1. Providing employees with computer access is one of the perks offered by your business. Employees enjoy checking their personal email and surfing the Internet on their breaks. So far, computer access has been a cherished employee benefit. When you came into work this morning you found the following anonymous letter from one of your employees on your desk. "I received a highly inappropriate joke from a fellow employee that I found extremely offensive. The employee who sent the joke was Debbie Fernandez and I believe she should be reprimanded for her inappropriate actions. Signed—a disturbed employee." What would you do? What could you have done to ensure situations such as these would be easily handled if they did arise? What could you do to ensure such situations do not happen in the future and if they do all employees are aware of the ramifications of inappropriate emails? (Be sure to identify your business and the name of your company.)
2. The local community has always been a big part of your grandfather's business and he knew almost everyone in the community. Your grandfather attended all types of community events and would spend hours talking with friends and neighbors soliciting feedback and ideas on his business. As you know, data are important to any business. In fact, data are an essential business asset. You have decided to start tracking detailed customer information for all business events from fund-raising to promotions. Since you took over the business you have been collecting more and more event data to help you run marketing campaigns across events and optimize the event schedules. One day, a sophisticated businessman walks into your business and asks to speak to the owner. He introduces himself as Lance Smith and says that he would like to talk to you in private. Smith is retiring and is closing his business that was located just down the street, and he wants to sell you his detailed customer information. Smith would like a large sum of money to sell you his confidential customer contact information and sales reports for the past 20 years. He says he has more than 10,000 customers in his unique database. What do you do?
3. Yesterday you had an interesting conversation with one of your loyal customers, Dan Martello. He asked you the following question: "If I find a digital camera on the street is it OK to look at the contents, or am I invading the owner's privacy?" You have a lengthy debate and decided that in some scenarios it is an invasion of privacy to be looking at someone else's photos and is similar to looking in their windows. In other scenarios, it is not an invasion of privacy if you do not know the person and it is the primary way to identify the owner to return the camera, similar to looking in a wallet. As you are cleaning your business, you find a 30 gigabyte thumb drive and you know that it probably belongs to one of your valuable customers and contains their sensitive information. What do you do? What security concerns are associated with the thumb drive? How could information security policies or an information security plan help your business with this type of situation?

PROJECT I Grading Security

Making The Grade is a nonprofit organization that helps students learn how to achieve better grades in school. The organization has 40 offices in 25 states and more than 2,000 employees. The company wants to build a website to offer its services online. Making The Grade's online services will provide parents seven key pieces of advice for communicating with their children to help them achieve academic success. The website will offer information on how to maintain open lines of communication, set goals, organize academics, regularly track progress, identify trouble spots, get to know their child's teacher, and celebrate their children's successes.

Project Focus

You and your team work for the director of information security. Your team's assignment is to develop a document discussing the importance of creating information security polices and an information security plan. Be sure to include the following:

- The importance of educating employees on information security.
- A few samples of employee information security policies specifically for Making The Grade.
- Other major areas the information security plan should address.
- Signs the company should look for to determine if the website is being hacked.
- The major types of attacks the company should expect to experience.

PROJECT II Eyes Everywhere

The movie *Minority Report* chronicled a futuristic world where people are uniquely identifiable by their eyes. A scan of each person's eyes gives or denies them access to rooms, computers, and anything else with restrictions. The movie portrayed a black market in new eyeballs to help people hide from the authorities. (Why did they not just change the database entry instead? That would have been much easier, but a lot less dramatic.)

The idea of using a biological signature is entirely plausible because biometrics is currently being used and is expected to gain wider acceptance in the near future because forging documents has become much easier with the advances in computer graphics programs and color printers. The next time you get a new passport, it may incorporate a chip that has your biometric information encoded on it. Office of Special Investigations agents with fake documents found that it was relatively easy to enter the United States from Canada, Mexico, and Jamaica, by land, sea, and air.

The task of policing the borders is daunting. Some 500 million foreigners enter the country every year and go through identity checkpoints. More than 13 million permanent-resident and border-crossing cards have been issued by the U.S. government. Also, citizens of 27 countries do not need visas to enter this country. They are expected to have passports that comply with U.S. specifications that will also be readable at the border.

In the post-9/11 atmosphere of tightened security, unrestricted border crossing is not acceptable. The Department of Homeland Security is charged with securing the nation's borders, and as part of this plan, new entry/exit procedures were instituted at the beginning of 2003. An integrated system, using biometrics, will be used to identify foreign visitors to the United States and reduce the likelihood of terrorists entering the country.

Early in 2003, after 6 million biometric border-crossing cards had been issued, a pilot test conducted at the Canadian border detected more than 250 imposters. The testing started with

two biometric identifiers: photographs for facial recognition and fingerprint scans. As people enter and leave the country, their actual fingerprints and facial features are compared to the data on the biometric chip in the passport.

Project Focus

In a group, discuss the following:

a. How do you feel about having your fingerprints, facial features, and perhaps more of your biometric features encoded in documents such as your passport? Explain your answer.

b. Would you feel the same way about having biometric information on your driver's license as on your passport? Why or why not?

c. Is it reasonable to have different biometric identification requirements for visitors from different nations? Explain your answer. What would you recommend as criteria for deciding which countries fall into what categories?

d. The checkpoints U.S. citizens pass through upon returning to the country vary greatly in the depth of the checks and the time spent. The simplest involves simply walking past the border guards who may or may not ask you your citizenship. The other end of the spectrum requires that you put up with long waits in airports where you have to line up with hundreds of other passengers while each person is questioned and must produce a passport to be scanned. Would you welcome biometric information on passports if it would speed the process, or do you think that the disadvantages of the reduction in privacy, caused by biometric information, outweigh the advantages of better security and faster border processing? Explain your answer.

PROJECT III Setting Boundaries

Even the most ethical people sometimes face difficult choices. Acting ethically means behaving in a principled fashion and treating other people with respect and dignity. It is simple to say, but not so simple to do since some situations are complex or ambiguous. The important role of ethics in our lives has long been recognized. As far back as 44 B.C., Cicero said that ethics are indispensable to anyone who wants to have a good career. Having said that, Cicero, along with some of the greatest minds over the centuries, struggled with what the rules of ethics should be.

Our ethics are rooted in our history, culture, and religion, and our sense of ethics may shift over time. The electronic age brings with it a new dimension in the ethics debate—the amount of personal information that we can collect and store, and the speed with which we can access and process that information.

Project Focus

In a group, discuss how you would react to the following situations:

a. A senior marketing manager informs you that one of her employees is looking for another job and she wants you to give her access to look through her email.

b. A vice president of sales informs you that he has made a deal to provide customer information to a strategic partner, and he wants you to copy all of the customer information to a thumb drive.

c. You are asked to monitor your employee's email to discover whether he is sexually harassing another employee.

d. You are asked to install a video surveillance system in your office to find out whether employees are taking office supplies home with them.

e. You are looking on the shared network drive and discover that your boss's entire hard drive has been copied to the network for everyone to view. What do you do?

f. You have been accidentally copied on an email from the CEO, which details who will be the targets of the next round of layoffs. What do you do?

PROJECT IV Contemplating Sharing

Bram Cohen created BitTorrent which allows users to upload and download large amounts of data. Cohen demonstrated his program at the world hacker conference, as a free, open source project aimed at computer users who need a cheap way to swap software online. Soon many TV and movie fanatics began using the program to download copyrighted materials. As a result of the hacker conference, more than 20 million people downloaded the BitTorrent program and began sharing movies and television shows across the Internet.

Project Focus

There is much debate surrounding the ethics of peer-to-peer networking. Do you believe BitTorrent is ethical or unethical? Justify your answer.

AYK APPLICATION PROJECTS

If you are looking for Excel projects to incorporate into your class, try any of the following after reading this chapter.

Project Number	Project Name	Project Type	Plug-In Focus Area	Project Focus	Project Skill Set	Page Number
1	Financial Destiny	Excel	T2	Personal Budget	Introductory Formulas	AYK.4
2	Cash Flow	Excel	T2	Cash Flow	Introductory Formulas	AYK.4
3	Technology Budget	Excel	T1, T2	Hardware and Software	Introductory Formulas	AYK.4
4	Tracking Donations	Excel	T2	Employee Relationships	Introductory Formulas	AYK.4
5	Convert Currency	Excel	T2	Global Commerce	Introductory Formulas	AYK.5
6	Cost Comparison	Excel	T2	Total Cost of Ownership	Introductory Formulas	AYK.5
7	Time Management	Excel or Project	T2 or T12	Project Management	Introductory Gantt Charts	AYK.6
8	Maximize Profit	Excel	T2, T4	Strategic Analysis	Intermediate Formulas or Solver	AYK.6
9	Security Analysis	Excel	T3	Filtering Data	Intermediate Conditional Formatting, Autofilter, Subtotal	AYK.7
10	Gathering Data	Excel	T3	Data Analysis	Intermediate Conditional Formatting, PivotTable	AYK.8
11	Scanner System	Excel	T2	Strategic Analysis	Intermediate	AYK.8
12	Competitive Pricing	Excel	T2	Profit Maximization	Intermediate	AYK.9
13	Adequate Acquisitions	Excel	T2	Break-Even Analysis	Intermediate	AYK.9
24	Electronic Resumes	HTML	T9, T10, T11	Electronic Personal Marketing	Introductory Structural Tags	AYK.16
25	Gathering Feedback	Dreamweaver	T9, T10, T11	Data Collection	Intermediate Organization of Information	AYK.16

Technical Foundations of MIS

module 2

Module 2 concentrates on the technical foundations of MIS. The power of MIS comes from its ability to carry, house, and support information. And information is power to an organization. This module highlights this point and raises awareness of the significance of information to organizational success. Understanding how the MIS infrastructure supports business operations, how business professionals access and analyze information to make business decisions, and how wireless and mobile technologies can make information continuously and instantaneously available are important for strategically managing any company, large or small. Thus, these are the primary learning outcomes of Module 2.

The module begins by reviewing the role of MIS in supporting business growth, operations, and performance. We quickly turn to the need for MIS to be sustainable given today's focus on being "green," and then dive into databases, data warehousing, networking, and wireless technologies—all fundamental components of MIS infrastructures. A theme throughout the module is the need to leverage and yet safeguard the use of information as key to the survival of any company. Information must be protected from misuse and harm, especially with the continued use, development, and exploitation of the Internet and the Web.

MODULE ONE:
Business Driven MIS

MODULE TWO:
Technical Foundations of MIS

MODULE THREE:
Enterprise MIS

Module 2: TECHNICAL FOUNDATIONS OF MIS