Chapter 8

Securing Information Systems

LEARNING OBJECTIVES

After reading this chapter, you will be able to answer the following questions:

1. Why are information systems vulnerable to destruction, error, and abuse?
2. What is the business value of security and control?
3. What are the components of an organizational framework for security and control?
4. What are the most important tools and technologies for safeguarding information resources?

Interactive Sessions:

When Antivirus Software Cripples Your Computers

How Secure Is the Cloud?

CHAPTER OUTLINE

YOU'RE ON FACEBOOK? WATCH OUT!

Facebook is the world's largest online social network, and increasingly, the destination of choice for messaging friends, sharing photos and videos, and collecting "eyeballs" for business advertising and market research. But, watch out! It's also a great place for losing your identity or being attacked by malicious software.

How could that be? Facebook has a security team that works hard to counter threats on that site. It uses up-to-date security technology to protect its Web site. But with 500 million users, it can't police everyone and everything. And Facebook makes an extraordinarily tempting target for both mischief-makers and criminals.

Facebook has a huge worldwide user base, an easy-to-use Web site, and a community of users linked to their friends. Its members are more likely to trust messages they receive from friends, even if this communication is not legitimate. Perhaps for these reasons, research from the Kaspersky Labs security firm shows malicious software on social networking sites such as Facebook and MySpace is 10 times more successful at infecting users than e-mail-based attacks. Moreover, IT security firm Sophos reported on February 1, 2010, that Facebook poses the greatest security risk of all the social networking sites.

Here are some examples of what can go wrong:

According to a February 2010 report from Internet security company NetWitness, Facebook served as the primary delivery method for an 18-month-long hacker attack in which Facebook users were tricked into revealing their passwords and downloading a rogue program that steals financial data. A legitimate-looking Facebook e-mail notice asked users to provide information to help the social network update its login system. When the user clicked the "update" button in the e-mail, that person was directed to a bogus Facebook login screen where the user's name was filled in and that person was prompted to provide his or her password. Once the user supplied that information, an "Update Tool," installed the Zeus "Trojan horse" rogue software program designed to steal financial and personal data by surreptitiously tracking users' keystrokes as they enter information into their computers. The hackers, most likely an Eastern European criminal group, stole as many as 68,000 login credentials from 2,400 companies and government agencies for online banking, social networking sites, and e-mail.

The Koobface worm targets Microsoft Windows users of Facebook, Twitter, and other social networking Web sites in order to gather sensitive information from the victims such as credit card numbers. Koobface was first detected in December 2008. It spreads by delivering bogus Facebook messages to people who are "friends" of a Facebook user whose computer has already been infected. Upon receipt, the message directs the recipients to a third-party Web site, where they are prompted to download what is purported to be an update of the Adobe Flash player. If they download and execute the file, Koobface is able to infect their system and use the computer for more malicious work.

For much of May 2010, Facebook members and their

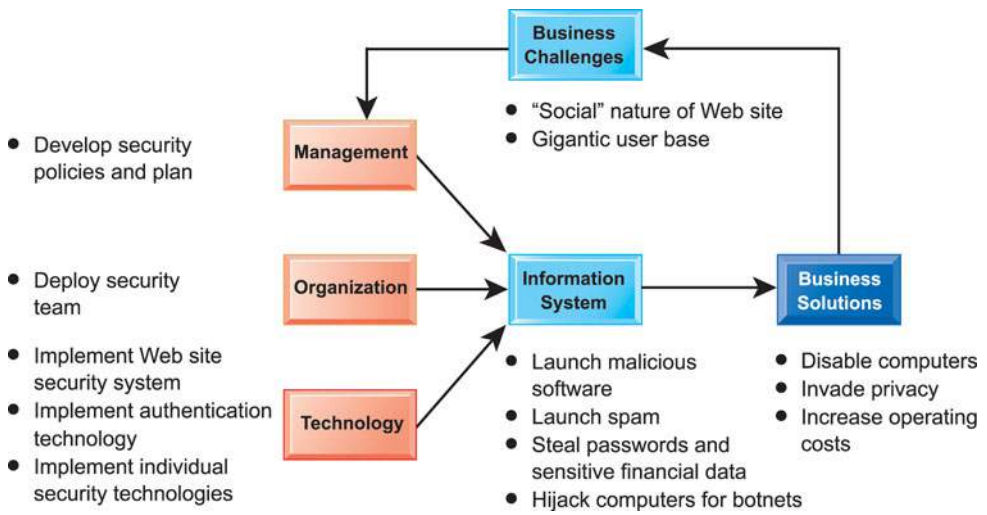
friends were victims of a spam campaign that tries to e-mail unsolicited advertisements and steal Facebook users' login credentials. The attack starts with a message containing a link to a bogus Web page sent by infected users to all of their friends. The message addresses each friend by name and invites that person to click on a link to "the most hilarious video ever." The link transports the user to a rogue Web site mimicking the Facebook login form. When users try to log in, the page redirects back to a Facebook application page that installs illicit adware software, which bombards their computers with all sorts of unwanted ads.

Recovering from these attacks is time-consuming and costly, especially for business firms. A September 2010 study by Panda Security found that one-third of small and medium businesses it surveyed had been hit by malicious software from social networks, and more than a third of these suffered more than $5,000 in losses. Of course, for large businesses, losses from Facebook are much greater.

Sources: Lance Whitney, "Social-Media Malware Hurting Small Businesses," CNET News, September 15, 2010; Raj Dash, "Report: Facebook Served as Primary Distribution Channel for Botnet Army," allfacebook.com, February 18, 2010; Sam Diaz, "Report: Bad Guys Go Social: Facebook Tops Security Risk List," *ZDNet*, February 1, 2010; Lucian Constantin, "Weekend Adware Scam Returns to Facebook," Softpedia, May 29, 2010; Brad Stone, "Viruses that Leave Victims Red in the Facebook," *The New York Times*, December 14, 2009; and Brian Prince, "Social Networks 10 Times as Effective for Hackers, Malware," *eWeek*, May 13, 2009.

The problems created by malicious software on Facebook illustrate some of the reasons why businesses need to pay special attention to information system security. Facebook provides a plethora of benefits to both individuals and businesses. But from a security standpoint, using Facebook is one of the easiest ways to expose a computer system to malicious software—your computer, your friends' computers, and even the computers of Facebook-participating businesses.

The chapter-opening diagram calls attention to important points raised by this case and this chapter. Although Facebook's management has a security policy and security team in place, Facebook has been plagued with many security problems that affect both individuals and businesses. The "social" nature of this site and large number of users make it unusually attractive for criminals and hackers intent on stealing valuable personal and financial information and propagating malicious software. Even though Facebook and its users deploy security technology, they are still vulnerable to new kinds of malicious software attacks and criminal scams. In addition to losses from theft of financial data, the difficulties of eradicating the malicious software or repairing damage caused by identity theft add to operational costs and make both individuals and businesses less effective.



8.1 System Vulnerability and Abuse

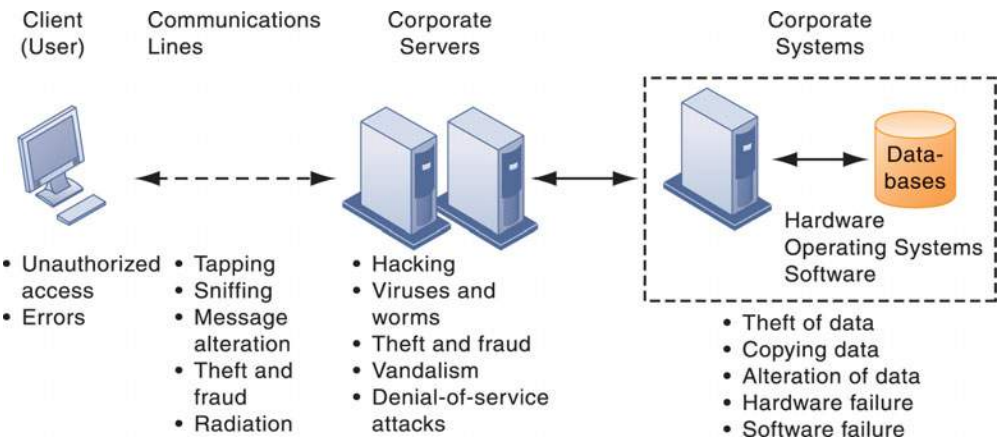
Can you imagine what would happen if you tried to link to the Internet without a firewall or antivirus software? Your computer would be disabled in a few seconds, and it might take you many days to recover. If you used the computer to run your business, you might not be able to sell to your customers or place orders with your suppliers while it was down. And you might find that your computer system had been penetrated by outsiders, who perhaps stole or destroyed valuable data, including confidential payment data from your customers. If too much data were destroyed or divulged, your business might never be able to operate!

In short, if you operate a business today, you need to make security and control a top priority. **Security** refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems. **Controls** are methods, policies, and organizational procedures that ensure the safety of the organization's assets; the accuracy and reliability of its records; and operational adherence to management standards.

WHY SYSTEMS ARE VULNERABLE

When large amounts of data are stored in electronic form, they are vulnerable to many more kinds of threats than when they existed in manual form. Through communications networks, information systems in different locations are interconnected. The potential for unauthorized access, abuse, or fraud is not limited to a single location but can occur at any access point in the network. Figure 8-1 illustrates the most common threats against contemporary information systems. They can stem from technical, organizational, and environmental factors compounded by poor management decisions. In the multi-tier client/server computing environment illustrated here, vulnerabilities exist at each layer and in the communications between the layers. Users at the client layer can cause harm by introducing errors or by accessing systems without

FIGURE 8-1 CONTEMPORARY SECURITY CHALLENGES AND VULNERABILITIES



The architecture of a Web-based application typically includes a Web client, a server, and corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities. Floods, fires, power failures, and other electrical problems can cause disruptions at any point in the network.

authorization. It is possible to access data flowing over networks, steal valuable data during transmission, or alter messages without authorization. Radiation may disrupt a network at various points as well. Intruders can launch denial-of-service attacks or malicious software to disrupt the operation of Web sites. Those capable of penetrating corporate systems can destroy or alter corporate data stored in databases or files.

Systems malfunction if computer hardware breaks down, is not configured properly, or is damaged by improper use or criminal acts. Errors in programming, improper installation, or unauthorized changes cause computer software to fail. Power failures, floods, fires, or other natural disasters can also disrupt computer systems.

Domestic or offshore partnering with another company adds to system vulnerability if valuable information resides on networks and computers outside the organization's control. Without strong safeguards, valuable data could be lost, destroyed, or could fall into the wrong hands, revealing important trade secrets or information that violates personal privacy.

The popularity of handheld mobile devices for business computing adds to these woes. Portability makes cell phones, smartphones, and tablet computers easy to lose or steal. Smartphones share the same security weaknesses as other Internet devices, and are vulnerable to malicious software and penetration from outsiders. In 2009, security experts identified 30 security flaws in software and operating systems of smartphones made by Apple, Nokia, and BlackBerry maker Research in Motion.

Even the apps that have been custom-developed for mobile devices are capable of turning into rogue software. For example, in December 2009, Google pulled dozens of mobile banking apps from its Android Market because they could have been updated to capture customers' banking credentials. Smartphones used by corporate executives may contain sensitive data such as sales figures, customer names, phone numbers, and e-mail addresses. Intruders may be able to access internal corporate networks through these devices.

Internet Vulnerabilities

Large public networks, such as the Internet, are more vulnerable than internal networks because they are virtually open to anyone. The Internet is so huge that when abuses do occur, they can have an enormously widespread impact. When the Internet becomes part of the corporate network, the organization's information systems are even more vulnerable to actions from outsiders.

Computers that are constantly connected to the Internet by cable modems or digital subscriber line (DSL) lines are more open to penetration by outsiders because they use fixed Internet addresses where they can be easily identified. (With dial-up service, a temporary Internet address is assigned for each session.) A fixed Internet address creates a fixed target for hackers.

Telephone service based on Internet technology (see Chapter 7) is more vulnerable than the switched voice network if it does not run over a secure private network. Most Voice over IP (VoIP) traffic over the public Internet is not encrypted, so anyone with a network can listen in on conversations. Hackers can intercept conversations or shut down voice service by flooding servers supporting VoIP with bogus traffic.

Vulnerability has also increased from widespread use of e-mail, instant messaging (IM), and peer-to-peer file-sharing programs. E-mail may contain attachments that serve as springboards for malicious software or unauthorized access to internal corporate systems. Employees may use e-mail messages to transmit valuable trade secrets, financial data, or confidential customer informa-

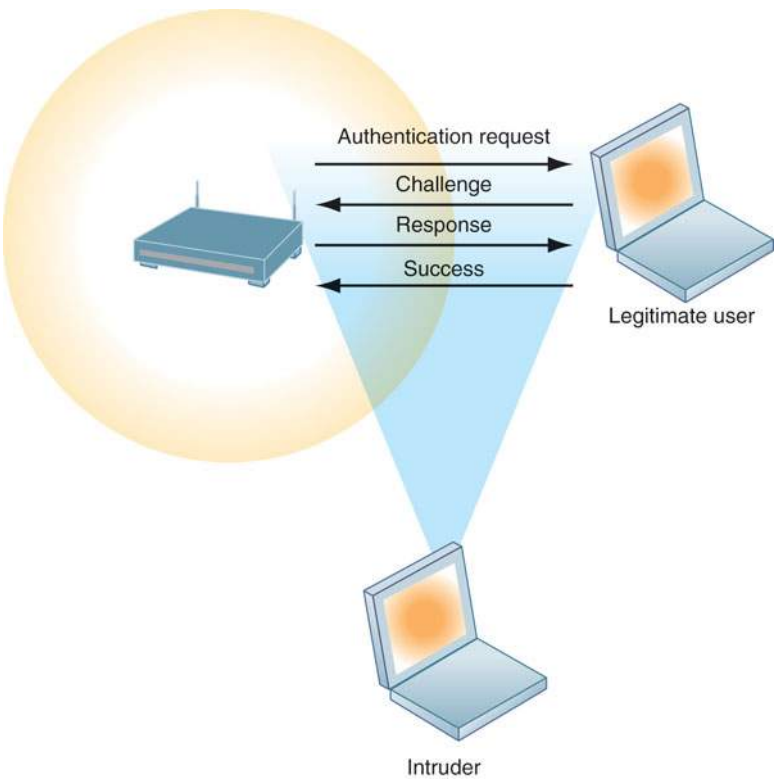
tion to unauthorized recipients. Popular IM applications for consumers do not use a secure layer for text messages, so they can be intercepted and read by outsiders during transmission over the public Internet. Instant messaging activity over the Internet can in some cases be used as a back door to an otherwise secure network. Sharing files over peer-to-peer (P2P) networks, such as those for illegal music sharing, may also transmit malicious software or expose information on either individual or corporate computers to outsiders.

Wireless Security Challenges

Is it safe to log onto a wireless network at an airport, library, or other public location? It depends on how vigilant you are. Even the wireless network in your home is vulnerable because radio frequency bands are easy to scan. Both Bluetooth and Wi-Fi networks are susceptible to hacking by eavesdroppers. Although the range of Wi-Fi networks is only several hundred feet, it can be extended up to one-fourth of a mile using external antennae. Local area networks (LANs) using the 802.11 standard can be easily penetrated by outsiders armed with laptops, wireless cards, external antennae, and hacking software. Hackers use these tools to detect unprotected networks, monitor network traffic, and, in some cases, gain access to the Internet or to corporate networks.

Wi-Fi transmission technology was designed to make it easy for stations to find and hear one another. The *service set identifiers (SSIDs)* identifying the access points in a Wi-Fi network are broadcast multiple times and can be picked up fairly easily by intruders' sniffer programs (see Figure 8-2). Wireless networks in many locations do not have basic protections against **war driving**,

FIGURE 8-2 WI-FI SECURITY CHALLENGES



Many Wi-Fi networks can be penetrated easily by intruders using sniffer programs to obtain an address to access the resources of a network without authorization.

in which eavesdroppers drive by buildings or park outside and try to intercept wireless network traffic.

A hacker can employ an 802.11 analysis tool to identify the SSID. (Windows XP, Vista, and 7 have capabilities for detecting the SSID used in a network and automatically configuring the radio NIC within the user's device.) An intruder that has associated with an access point by using the correct SSID is capable of accessing other resources on the network, using the Windows operating system to determine which other users are connected to the network, access their computer hard drives, and open or copy their files.

Intruders also use the information they have gleaned to set up rogue access points on a different radio channel in physical locations close to users to force a user's radio NIC to associate with the rogue access point. Once this association occurs, hackers using the rogue access point can capture the names and passwords of unsuspecting users.

The initial security standard developed for Wi-Fi, called Wired Equivalent Privacy (WEP), is not very effective. WEP is built into all standard 802.11 products, but its use is optional. Many users neglect to use WEP security features, leaving them unprotected. The basic WEP specification calls for an access point and all of its users to share the same 40-bit encrypted password, which can be easily decrypted by hackers from a small amount of traffic. Stronger encryption and authentication systems are now available, such as Wi-Fi Protected Access 2 (WPA2), but users must be willing to install them.

MALICIOUS SOFTWARE: VIRUSES, WORMS, TROJAN HORSES, AND SPYWARE

Malicious software programs are referred to as **malware** and include a variety of threats, such as computer viruses, worms, and Trojan horses. A **computer virus** is a rogue software program that attaches itself to other software programs or data files in order to be executed, usually without user knowledge or permission. Most computer viruses deliver a "payload." The payload may be relatively benign, such as the instructions to display a message or image, or it may be highly destructive—destroying programs or data, clogging computer memory, reformatting a computer's hard drive, or causing programs to run improperly. Viruses typically spread from computer to computer when humans take an action, such as sending an e-mail attachment or copying an infected file.

Most recent attacks have come from **worms**, which are independent computer programs that copy themselves from one computer to other computers over a network. (Unlike viruses, they can operate on their own without attaching to other computer program files and rely less on human behavior in order to spread from computer to computer. This explains why computer worms spread much more rapidly than computer viruses.) Worms destroy data and programs as well as disrupt or even halt the operation of computer networks.

Worms and viruses are often spread over the Internet from files of downloaded software, from files attached to e-mail transmissions, or from compromised e-mail messages or instant messaging. Viruses have also invaded computerized information systems from "infected" disks or infected machines. E-mail worms are currently the most problematic.

Malware targeting mobile devices is not as extensive as that targeting computers, but is spreading nonetheless using e-mail, text messages, Bluetooth,

and file downloads from the Web via Wi-Fi or cellular networks.There are now more than 200 viruses and worms targeting mobile phones, such as Cabir, Commwarrior, Frontal.A, and Ikee.B. Frontal.A installs a corrupted file that causes phone failure and prevents the user from rebooting, while Ikee.B turns jailbroken iPhones into botnet-controlled devices. Mobile device viruses pose serious threats to enterprise computing because so many wireless devices are now linked to corporate information systems.

Web 2.0 applications, such as blogs, wikis, and social networking sites such as Facebook and MySpace, have emerged as new conduits for malware or spyware. These applications allow users to post software code as part of the permissible content, and such code can be launched automatically as soon as a Web page is viewed. The chapter-opening case study describes other channels for malware targeting Facebook. In September 2010, hackers exploited a Twitter security flaw to send users to Japanese pornographic sites and automatically generated messages from other accounts (Coopes, 2010).

Table 8-1 describes the characteristics of some of the most harmful worms and viruses that have appeared to date.

Over the past decade, worms and viruses have caused billions of dollars of damage to corporate networks, e-mail systems, and data. According to Consumer Reports' State of the Net 2010 survey, U.S. consumers lost $3.5 billion

TABLE 8-1 EXAMPLES OF MALICIOUS CODE

NAME	TYPE	DESCRIPTION
Conficker (aka Downadup, Downup)	Worm	First detected in November 2008. Uses flaws in Windows software to take over machines and link them into a virtual computer that can be commanded remotely. Has more than 5 million computers worldwide under its control. Difficult to eradicate.
Storm	Worm/ Trojan horse	First identified in January 2007. Spreads via e-mail spam with a fake attachment. Infected up to 10 million computers, causing them to join its zombie network of computers engaged in criminal activity.
Sasser.ftp	Worm	First appeared in May 2004. Spread over the Internet by attacking random IP addresses. Causes computers to continually crash and reboot, and infected computers to search for more victims. Affected millions of computers worldwide, disrupting British Airways flight check-ins, operations of British coast guard stations, Hong Kong hospitals, Taiwan post office branches, and Australia's Westpac Bank. Sasser and its variants caused an estimated $14.8 billion to $18.6 billion in damages worldwide.
MyDoom.A	Worm	First appeared on January 26, 2004. Spreads as an e-mail attachment. Sends e-mail to addresses harvested from infected machines, forging the sender's address. At its peak this worm lowered global Internet performance by 10 percent and Web page loading times by as much as 50 percent. Was programmed to stop spreading after February 12, 2004.
Sobig.F	Worm	First detected on August 19, 2003. Spreads via e-mail attachments and sends massive amounts of mail with forged sender information. Deactivated itself on September 10, 2003, after infecting more than 1 million PCs and doing $5 to $10 billion in damage.
ILOVEYOU	Virus	First detected on May 3, 2000. Script virus written in Visual Basic script and transmitted as an attachment to e-mail with the subject line ILOVEYOU. Overwrites music, image, and other files with a copy of itself and did an estimated $10 billion to $15 billion in damage.
Melissa	Macro virus/ worm	First appeared in March 1999. Word macro script mailing infected Word file to first 50 entries in user's Microsoft Outlook address book. Infected 15 to 29 percent of all business PCs, causing $300 million to $600 million in damage.

because of malware and online scams, and the majority of these losses came from malware (Consumer Reports, 2010).

A **Trojan horse** is a software program that appears to be benign but then does something other than expected, such as the Zeus Trojan described in the chapter-opening case. The Trojan horse is not itself a virus because it does not replicate, but it is often a way for viruses or other malicious code to be introduced into a computer system. The term *Trojan horse* is based on the huge wooden horse used by the Greeks to trick the Trojans into opening the gates to their fortified city during the *Trojan War*. Once inside the city walls, Greek soldiers hidden in the horse revealed themselves and captured the city.

At the moment, **SQL injection attacks** are the largest malware threat. SQL injection attacks take advantage of vulnerabilities in poorly coded Web application software to introduce malicious program code into a company's systems and networks. These vulnerabilities occur when a Web application fails to properly validate or filter data entered by a user on a Web page, which might occur when ordering something online. An attacker uses this input validation error to send a rogue SQL query to the underlying database to access the database, plant malicious code, or access other systems on the network. Large Web applications have hundreds of places for inputting user data, each of which creates an opportunity for an SQL injection attack.

A large number of Web-facing applications are believed to have SQL injection vulnerabilities, and tools are available for hackers to check Web applications for these vulnerabilities. Such tools are able to locate a data entry field on a Web page form, enter data into it, and check the response to see if shows vulnerability to a SQL injection.

Some types of spyware also act as malicious software. These small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising. Thousands of forms of spyware have been documented.

Many users find such **spyware** annoying and some critics worry about its infringement on computer users' privacy. Some forms of spyware are especially nefarious. **Keyloggers** record every keystroke made on a computer to steal serial numbers for software, to launch Internet attacks, to gain access to e-mail accounts, to obtain passwords to protected computer systems, or to pick up personal information such as credit card numbers. Other spyware programs reset Web browser home pages, redirect search requests, or slow performance by taking up too much memory. The Zeus Trojan described in the chapter-opening case uses keylogging to steal financial information.

HACKERS AND COMPUTER CRIME

A **hacker** is an individual who intends to gain unauthorized access to a computer system. Within the hacking community, the term *cracker* is typically used to denote a hacker with criminal intent, although in the public press, the terms hacker and cracker are used interchangeably. Hackers and crackers gain unauthorized access by finding weaknesses in the security protections employed by Web sites and computer systems, often taking advantage of various features of the Internet that make it an open system that is easy to use.

Hacker activities have broadened beyond mere system intrusion to include theft of goods and information, as well as system damage and **cybervandalism**, the intentional disruption, defacement, or even destruction of a Web site or corporate information system. For example, cybervandals have turned many of the MySpace "group" sites, which are dedicated to interests such as home beer

brewing or animal welfare, into cyber-graffiti walls, filled with offensive comments and photographs.

Spoofing and Sniffing

Hackers attempting to hide their true identities often spoof, or misrepresent, themselves by using fake e-mail addresses or masquerading as someone else. **Spoofing** also may involve redirecting a Web link to an address different from the intended one, with the site masquerading as the intended destination. For example, if hackers redirect customers to a fake Web site that looks almost exactly like the true site, they can then collect and process orders, effectively stealing business as well as sensitive customer information from the true site. We provide more detail on other forms of spoofing in our discussion of computer crime.

A **sniffer** is a type of eavesdropping program that monitors information traveling over a network. When used legitimately, sniffers help identify potential network trouble spots or criminal activity on networks, but when used for criminal purposes, they can be damaging and very difficult to detect. Sniffers enable hackers to steal proprietary information from anywhere on a network, including e-mail messages, company files, and confidential reports.

Denial-of-Service Attacks

In a **denial-of-service (DoS) attack**, hackers flood a network server or Web server with many thousands of false communications or requests for services to crash the network. The network receives so many queries that it cannot keep up with them and is thus unavailable to service legitimate requests. A **distributed denial-of-service (DDoS)** attack uses numerous computers to inundate and overwhelm the network from numerous launch points.

For example, during the 2009 Iranian election protests, foreign activists trying to help the opposition engaged in DDoS attacks against Iran's government. The official Web site of the Iranian government (ahmadinejad.ir) was rendered inaccessible on several occasions.

Although DoS attacks do not destroy information or access restricted areas of a company's information systems, they often cause a Web site to shut down, making it impossible for legitimate users to access the site. For busy e-commerce sites, these attacks are costly; while the site is shut down, customers cannot make purchases. Especially vulnerable are small and midsize businesses whose networks tend to be less protected than those of large corporations.

Perpetrators of DoS attacks often use thousands of "zombie" PCs infected with malicious software without their owners' knowledge and organized into a **botnet**. Hackers create these botnets by infecting other people's computers with bot malware that opens a back door through which an attacker can give instructions. The infected computer then becomes a slave, or zombie, serving a master computer belonging to someone else. Once a hacker infects enough computers, her or she can use the amassed resources of the botnet to launch DDos attacks, phishing campaigns, or unsolicited "spam" e-mail.

The number of computers that are part of botnets is variously estimated to be from 6 to 24 million, with thousands of botnets operating worldwide. The largest botnet attack in 2010 was the Mariposa botnet, which started in Spain and spread across the world. Mariposa had infected and controlled about 12.7 million computers in its efforts to steal credit card numbers and online banking passwords. More than half the Fortune 1000 companies, 40 major banks, and numerous government agencies were infected—and did not know it.

The chapter-ending case study describes multiple waves of DDoS attacks targeting a number of Web sites of government agencies and other organizations in South Korea and the United States in July 2009. The attacker used a botnet controlling over 65,000 computers, and was able to cripple some of these sites for several days. Most of the botnet originated from China, and North Korea. Botnet attacks thought to have originated in Russia were responsible for crippling the Web sites of the Estonian government in April 2007 and the Georgian government in July 2008.

Computer Crime

Most hacker activities are criminal offenses, and the vulnerabilities of systems we have just described make them targets for other types of **computer crime** as well. For example, in early July 2009, U.S. federal agents arrested Sergey Aleynikov, a computer programmer at investment banking firm Goldman Sachs, for stealing proprietary computer programs used in making lucrative rapid-fire trades in the financial markets. The software brought Goldman many millions of dollars of profits per year and, in the wrong hands, could have been used to manipulate financial markets in unfair ways. Computer crime is defined by the U.S. Department of Justice as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution." Table 8-2 provides examples of the computer as a target of crime and as an instrument of crime.

No one knows the magnitude of the computer crime problem—how many systems are invaded, how many people engage in the practice, or the total economic damage. According to the 2009 CSI Computer Crime and Security Survey of 500 companies, participants' average annual loss from computer crime and security attacks was close to $234,000 (Computer Security Institute, 2009). Many companies are reluctant to report computer crimes because the crimes may involve employees, or the company fears that publicizing its vulnerability will hurt its reputation. The most economically damaging kinds of computer crime are

TABLE 8-2 EXAMPLES OF COMPUTER CRIME

COMPUTERS AS TARGETS OF CRIME
Breaching the confidentiality of protected computerized data
Accessing a computer system without authority
Knowingly accessing a protected computer to commit fraud
Intentionally accessing a protected computer and causing damage, negligently or deliberately
Knowingly transmitting a program, program code, or command that intentionally causes damage to a protected computer
Threatening to cause damage to a protected computer
COMPUTERS AS INSTRUMENTS OF CRIME
Theft of trade secrets
Unauthorized copying of software or copyrighted intellectual property, such as articles, books, music, and video
Schemes to defraud
Using e-mail for threats or harassment
Intentionally attempting to intercept electronic communication
Illegally accessing stored electronic communications, including e-mail and voice mail
Transmitting or possessing child pornography using a computer

DoS attacks, introducing viruses, theft of services, and disruption of computer systems.

Identity Theft

With the growth of the Internet and electronic commerce, identity theft has become especially troubling. **Identity theft** is a crime in which an imposter obtains key pieces of personal information, such as social security identification numbers, driver's license numbers, or credit card numbers, to impersonate someone else. The information may be used to obtain credit, merchandise, or services in the name of the victim or to provide the thief with false credentials. According to Javelin Strategy and Research, losses from identity theft rose to $54 billion in 2009, and over 11 million U.S. adults were victims of identity fraud (Javelin Strategy & Research, 2010).

Identify theft has flourished on the Internet, with credit card files a major target of Web site hackers. Moreover, e-commerce sites are wonderful sources of customer personal information—name, address, and phone number. Armed with this information, criminals are able to assume new identities and establish new credit for their own purposes.

One increasingly popular tactic is a form of spoofing called **phishing**. Phishing involves setting up fake Web sites or sending e-mail or text messages that look like those of legitimate businesses to ask users for confidential personal data. The message instructs recipients to update or confirm records by providing social security numbers, bank and credit card information, and other confidential data either by responding to the e-mail message, by entering the information at a bogus Web site, or by calling a telephone number. EBay, PayPal, Amazon.com, Walmart, and a variety of banks, are among the top spoofed companies.

New phishing techniques called evil twins and pharming are harder to detect. **Evil twins** are wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet, such as those in airport lounges, hotels, or coffee shops. The bogus network looks identical to a legitimate public network. Fraudsters try to capture passwords or credit card numbers of unwitting users who log on to the network.

Pharming redirects users to a bogus Web page, even when the individual types the correct Web page address into his or her browser. This is possible if pharming perpetrators gain access to the Internet address information stored by Internet service providers to speed up Web browsing and the ISP companies have flawed software on their servers that allows the fraudsters to hack in and change those addresses.

In the largest instance of identity theft to date, Alberto Gonzalez of Miami and two Russian co-conspirators penetrated the corporate systems of TJX Corporation, Hannaford Brothers, 7-Eleven, and other major retailers, stealing over 160 million credit and debit card numbers between 2005 and 2008. The group initially planted "sniffer" programs in these companies' computer networks that captured card data as they were being transmitted between computer systems. They later switched to SQL injection attacks, which we introduced earlier in this chapter, to penetrate corporate databases. In March 2010, Gonzalez was sentenced to 20 years in prison. TJX alone spent over $200 million to deal with its data theft, including legal settlements.

The U.S. Congress addressed the threat of computer crime in 1986 with the Computer Fraud and Abuse Act. This act makes it illegal to access a computer system without authorization. Most states have similar laws, and nations in Europe have comparable legislation. Congress also passed the National Information Infrastructure Protection Act in 1996 to make virus distribution

and hacker attacks that disable Web sites federal crimes. U.S. legislation, such as the Wiretap Act, Wire Fraud Act, Economic Espionage Act, Electronic Communications Privacy Act, E-mail Threats and Harassment Act, and Child Pornography Act, covers computer crimes involving intercepting electronic communication, using electronic communication to defraud, stealing trade secrets, illegally accessing stored electronic communications, using e-mail for threats or harassment, and transmitting or possessing child pornography.

Click Fraud

When you click on an ad displayed by a search engine, the advertiser typically pays a fee for each click, which is supposed to direct potential buyers to its products. **Click fraud** occurs when an individual or computer program fraudulently clicks on an online ad without any intention of learning more about the advertiser or making a purchase. Click fraud has become a serious problem at Google and other Web sites that feature pay-per-click online advertising.

Some companies hire third parties (typically from low-wage countries) to fraudulently click on a competitor's ads to weaken them by driving up their marketing costs. Click fraud can also be perpetrated with software programs doing the clicking, and botnets are often used for this purpose. Search engines such as Google attempt to monitor click fraud but have been reluctant to publicize their efforts to deal with the problem.

Global Threats: Cyberterrorism and Cyberwarfare

The cybercriminal activities we have described—launching malware, denial-of-service attacks, and phishing probes—are borderless. Computer security firm Sophos reported that 42 percent of the malware it identified in early 2010 originated in the United States, while 11 percent came from China, and 6 percent from Russia (Sophos, 2010). The global nature of the Internet makes it possible for cybercriminals to operate—and to do harm—anywhere in the world.

Concern is mounting that the vulnerabilities of the Internet or other networks make digital networks easy targets for digital attacks by terrorists, foreign intelligence services, or other groups seeking to create widespread disruption and harm. Such cyberattacks might target the software that runs electrical power grids, air traffic control systems, or networks of major banks and financial institutions. At least 20 countries, including China, are believed to be developing offensive and defensive cyberwarfare capabilities. The chapter-ending case study discusses this problem in greater detail.

INTERNAL THREATS: EMPLOYEES

We tend to think the security threats to a business originate outside the organization. In fact, company insiders pose serious security problems. Employees have access to privileged information, and in the presence of sloppy internal security procedures, they are often able to roam throughout an organization's systems without leaving a trace.

Studies have found that user lack of knowledge is the single greatest cause of network security breaches. Many employees forget their passwords to access computer systems or allow co-workers to use them, which compromises the system. Malicious intruders seeking system access sometimes trick employees into revealing their passwords by pretending to be legitimate members of the company in need of information. This practice is called **social engineering**.

Both end users and information systems specialists are also a major source of errors introduced into information systems. End users introduce errors by

entering faulty data or by not following the proper instructions for processing data and using computer equipment. Information systems specialists may create software errors as they design and develop new software or maintain existing programs.

SOFTWARE VULNERABILITY

Software errors pose a constant threat to information systems, causing untold losses in productivity. Growing complexity and size of software programs, coupled with demands for timely delivery to markets, have contributed to an increase in software flaws or vulnerabilities For example, a database-related software error prevented millions of JP Morgan Chase retail and small-business customers from accessing their online bank accounts for two days in September 2010 (Dash, 2010).

A major problem with software is the presence of hidden **bugs** or program code defects. Studies have shown that it is virtually impossible to eliminate all bugs from large programs. The main source of bugs is the complexity of decision-making code. A relatively small program of several hundred lines will contain tens of decisions leading to hundreds or even thousands of different paths. Important programs within most corporations are usually much larger, containing tens of thousands or even millions of lines of code, each with many times the choices and paths of the smaller programs.

Zero defects cannot be achieved in larger programs. Complete testing simply is not possible. Fully testing programs that contain thousands of choices and millions of paths would require thousands of years. Even with rigorous testing, you would not know for sure that a piece of software was dependable until the product proved itself after much operational use.

Flaws in commercial software not only impede performance but also create security vulnerabilities that open networks to intruders. Each year security firms identify thousands of software vulnerabilities in Internet and PC software. For instance, in 2009, Symantec identified 384 browser vulnerabilities: 169 in Firefox, 94 in Safari, 45 in Internet Explorer, 41 in Chrome, and 25 in Opera. Some of these vulnerabilities were critical (Symantec, 2010).

To correct software flaws once they are identified, the software vendor creates small pieces of software called **patches** to repair the flaws without disturbing the proper operation of the software. An example is Microsoft's Windows Vista Service Pack 2, released in April 2009, which includes some security enhancements to counter malware and hackers. It is up to users of the software to track these vulnerabilities, test, and apply all patches. This process is called *patch management*.

Because a company's IT infrastructure is typically laden with multiple business applications, operating system installations, and other system services, maintaining patches on all devices and services used by a company is often time-consuming and costly. Malware is being created so rapidly that companies have very little time to respond between the time a vulnerability and a patch are announced and the time malicious software appears to exploit the vulnerability.

The need to respond so rapidly to the torrent of security vulnerabilities even creates defects in the software meant to combat them, including popular antivirus products. What happened in the spring of 2010 to McAfee, a leading vendor of commercial antivirus software is an example, as discussed in the Interactive Session on Management.

INTERACTIVE SESSION: MANAGEMENT

WHEN ANTIVIRUS SOFTWARE CRIPPLES YOUR COMPUTERS

McAfee is a prominent antivirus software and computer security company based in Santa Clara, California. Its popular VirusScan product (now named AntiVirus Plus) is used by companies and individual consumers across the world, driving its revenues of $1.93 billion in 2009.

A truly global company, McAfee has over 6,000 employees across North America, Europe, and Asia. VirusScan and other McAfee security products address endpoint security, network security, and risk and compliance. The company has worked to compile a long track record of good customer service and strong quality assurance.

At 6 a.m. PDT April 21, 2010, McAfee made a blunder that threatened to destroy that track record and prompted the possible departure of hundreds of valued customers. McAfee released what should have been a routine update for its flagship VirusScan product that was intended to deal with a powerful new virus known as 'W32/wecorl.a". Instead, McAfee's update caused potentially hundreds of thousands of McAfee-equipped machines running Windows XP to crash and fail to reboot. How could McAfee, a company whose focus is saving and preserving computers, commit a gaffe that accomplished the opposite for a significant portion of its client base?

That was the question McAfee's angry clients were asking on the morning of April 21, when their computers were crippled or totally non-functional. The updates mistakenly targeted a critical Windows file, svchost.exe, which hosts other services used by various programs on PCs. Usually, more than one instance of the process is running at any given time, and eliminating them all would cripple any system. Though many viruses, including W32/wecorl.a, disguise themselves using the name svchost.exe to avoid detection, McAfee had never had problems with viruses using that technique before.

To make matters worse, without svchost.exe, Windows computers can't boot properly. VirusScan users applied the update, tried rebooting their systems, and were powerless to act as their systems went haywire, repeatedly rebooting, losing their network capabilities and, worst of all, their ability to detect USB drives, which is the only way of fixing affected computers. Companies using McAfee and that relied heavily on Windows XP computers struggled to cope with the majority of their machines suddenly failing.

Angry network administrators turned to McAfee for answers, and the company was initially just as confused as its clients regarding how such a monumental slipup could occur. Soon, McAfee determined that the majority of affected machines were using Windows XP Service Pack 3 combined with McAfee VirusScan version 8.7. They also noted that the "Scan Processes on enable" option of VirusScan, off by default in most VirusScan installations, was turned on in the majority of affected computers.

McAfee conducted a more thorough investigation into its mistake and published a FAQ sheet that explained more completely why they had made such a big mistake and which customers were affected. The two most prominent points of failure were as follows: first, users should have received a warning that svchost.exe was going to be quarantined or deleted, instead of automatically disposing of the file. Next, McAfee's automated quality assurance testing failed to detect such a critical error because of what the company called "inadequate coverage of product and operating systems in the test systems used."

The only way tech support staffs working in organizations could fix the problem was to go from computer to computer manually. McAfee released a utility called "SuperDAT Remediation Tool," which had to be downloaded to an unaffected machine, placed on a flash drive, and run in Windows Safe Mode on affected machines. Because affected computers lacked network access, this had to be done one computer at a time until all affected machines were repaired. The total number of machines impacted is not known but it doubtless involved tens of thousands of corporate computers. Needless to say, network administrators and corporate tech support divisions were incensed.

Regarding the flaws in McAfee's quality assurance processes, the company explained in the FAQ that they had not included Windows XP Service Pack 3 with VirusScan version 8.7 in the test configuration of operating systems and McAfee product versions. This explanation flabbergasted many of McAfee's clients and other industry analysts, since XP SP3 is the most widely used desktop PC configuration.

Vista and Windows 7 generally ship with new computers and are rarely installed on functioning XP computers.

Another reason that the problem spread so quickly without detection was the increasing demand for faster antivirus updates. Most companies aggressively deploy their updates to ensure that machines spend as little time exposed to new viruses as possible. McAfee's update reached a large number of machines so quickly without detection because most companies trust their antivirus provider to get it right.

Unfortunately for McAfee, it only takes a single slipup or oversight to cause significant damage to an antivirus company's reputation. McAfee was criticized for its slow response to the crisis and for its initial attempts to downplay the issue's impact on its customers. The company released a statement claiming that only a small fraction of its customers were affected, but this was soon shown to be false. Two days after the update was released, McAfee executive Barry McPherson finally apologized to customers on the company's blog. Soon after, CEO David DeWalt recorded a video for customers, still available via McAfee's Web site, in which he apologized for and explained the incident.

Sources: Peter Svensson, "McAfee Antivirus Program Goes Berserk, Freezes PCs," Associated Press, April 21, 2010; Gregg Keizer, "McAfee Apologizes for Crippling PCs with Bad Update," *Computerworld*, April 23, 2010 and "McAfee Update Mess Explained," *Computerworld*, April 22, 2010; Ed Bott, "McAfee Admits 'Inadequate' Quality Control Caused PC Meltdown," *ZDNet*, April 22, 2010; and Barry McPherson, "An Update on False Positive Remediation," http://siblog.mcafee.com/support/an-update-on-false-positive-remediation, April 22, 2010.

CASE STUDY QUESTIONS

1. What management, organization, and technology factors were responsible for McAfee's software problem?
2. What was the business impact of this software problem, both for McAfee and for its customers?
3. If you were a McAfee enterprise customer, would you consider McAfee's response to the problem be acceptable? Why or why not?
4. What should McAfee do in the future to avoid similar problems?

MIS IN ACTION

Search online for the apology by Barry McPherson ("Barry McPherson apology") and read the reaction of customers. Do you think McPherson's apology helped or inflamed the situation? What is a "false positive remediation"?

8.2 Business Value of Security and Control

Many firms are reluctant to spend heavily on security because it is not directly related to sales revenue. However, protecting information systems is so critical to the operation of the business that it deserves a second look.

Companies have very valuable information assets to protect. Systems often house confidential information about individuals' taxes, financial assets, medical records, and job performance reviews. They also can contain information on corporate operations, including trade secrets, new product development plans, and marketing strategies. Government systems may store information on weapons systems, intelligence operations, and military targets. These information assets have tremendous value, and the repercussions can be devastating if they are lost, destroyed, or placed in the wrong hands. One study estimated that when the security of a large firm is compromised, the company loses approximately 2.1 percent of its market value within two days of the security breach, which translates into an average loss of $1.65 billion in stock market value per incident (Cavusoglu, Mishra, and Raghunathan, 2004).

Inadequate security and control may result in serious legal liability. Businesses must protect not only their own information assets but also those of customers, employees, and business partners. Failure to do so may open the firm to costly litigation for data exposure or theft. An organization can be held liable for needless risk and harm created if the organization fails to take appropriate protective action to prevent loss of confidential information, data corruption, or breach of privacy. For example, BJ's Wholesale Club was sued by the U.S. Federal Trade Commission for allowing hackers to access its systems and steal credit and debit card data for fraudulent purchases. Banks that issued the cards with the stolen data sought $13 million from BJ's to compensate them for reimbursing card holders for the fraudulent purchases. A sound security and control framework that protects business information assets can thus produce a high return on investment. Strong security and control also increase employee productivity and lower operational costs.

LEGAL AND REGULATORY REQUIREMENTS FOR ELECTRONIC RECORDS MANAGEMENT

Recent U.S. government regulations are forcing companies to take security and control more seriously by mandating the protection of data from abuse, exposure, and unauthorized access. Firms face new legal obligations for the retention and storage of electronic records as well as for privacy protection.

If you work in the health care industry, your firm will need to comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. **HIPAA** outlines medical security and privacy rules and procedures for simplifying the administration of health care billing and automating the transfer of health care data between health care providers, payers, and plans. It requires members of the health care industry to retain patient information for six years and ensure the confidentiality of those records. It specifies privacy, security, and electronic transaction standards for health care providers handling patient information, providing penalties for breaches of medical privacy, disclosure of patient records by e-mail, or unauthorized network access.

If you work in a firm providing financial services, your firm will need to comply with the Financial Services Modernization Act of 1999, better known as the **Gramm-Leach-Bliley Act** after its congressional sponsors. This act requires financial institutions to ensure the security and confidentiality of customer data. Data must be stored on a secure medium, and special security measures must be enforced to protect such data on storage media and during transmittal.

If you work in a publicly traded company, your company will need to comply with the Public Company Accounting Reform and Investor Protection Act of 2002, better known as the **Sarbanes-Oxley Act** after its sponsors Senator Paul Sarbanes of Maryland and Representative Michael Oxley of Ohio. This Act was designed to protect investors after the financial scandals at Enron, WorldCom, and other public companies. It imposes responsibility on companies and their management to safeguard the accuracy and integrity of financial information that is used internally and released externally. One of the Learning Tracks for this chapter discusses Sarbanes-Oxley in detail.

Sarbanes-Oxley is fundamentally about ensuring that internal controls are in place to govern the creation and documentation of information in financial

statements. Because information systems are used to generate, store, and transport such data, the legislation requires firms to consider information systems security and other controls required to ensure the integrity, confidentiality, and accuracy of their data. Each system application that deals with critical financial reporting data requires controls to make sure the data are accurate. Controls to secure the corporate network, prevent unauthorized access to systems and data, and ensure data integrity and availability in the event of disaster or other disruption of service are essential as well.

ELECTRONIC EVIDENCE AND COMPUTER FORENSICS

Security, control, and electronic records management have become essential for responding to legal actions. Much of the evidence today for stock fraud, embezzlement, theft of company trade secrets, computer crime, and many civil cases is in digital form. In addition to information from printed or typewritten pages, legal cases today increasingly rely on evidence represented as digital data stored on portable floppy disks, CDs, and computer hard disk drives, as well as in e-mail, instant messages, and e-commerce transactions over the Internet. E-mail is currently the most common type of electronic evidence.

In a legal action, a firm is obligated to respond to a discovery request for access to information that may be used as evidence, and the company is required by law to produce those data. The cost of responding to a discovery request can be enormous if the company has trouble assembling the required data or the data have been corrupted or destroyed. Courts now impose severe financial and even criminal penalties for improper destruction of electronic documents.

An effective electronic document retention policy ensures that electronic documents, e-mail, and other records are well organized, accessible, and neither retained too long nor discarded too soon. It also reflects an awareness of how to preserve potential evidence for computer forensics. **Computer forensics** is the scientific collection, examination, authentication, preservation, and analysis of data held on or retrieved from computer storage media in such a way that the information can be used as evidence in a court of law. It deals with the following problems:

- Recovering data from computers while preserving evidential integrity
- Securely storing and handling recovered electronic data
- Finding significant information in a large volume of electronic data
- Presenting the information to a court of law

Electronic evidence may reside on computer storage media in the form of computer files and as *ambient data*, which are not visible to the average user. An example might be a file that has been deleted on a PC hard drive. Data that a computer user may have deleted on computer storage media can be recovered through various techniques. Computer forensics experts try to recover such hidden data for presentation as evidence.

An awareness of computer forensics should be incorporated into a firm's contingency planning process. The CIO, security specialists, information systems staff, and corporate legal counsel should all work together to have a plan in place that can be executed if a legal need arises. You can find out more about computer forensics in the Learning Tracks for this chapter.

8.3 Establishing a Framework for Security and Control

Even with the best security tools, your information systems won't be reliable and secure unless you know how and where to deploy them. You'll need to know where your company is at risk and what controls you must have in place to protect your information systems. You'll also need to develop a security policy and plans for keeping your business running if your information systems aren't operational.

INFORMATION SYSTEMS CONTROLS

Information systems controls are both manual and automated and consist of both general controls and application controls. **General controls** govern the design, security, and use of computer programs and the security of data files in general throughout the organization's information technology infrastructure. On the whole, general controls apply to all computerized applications and consist of a combination of hardware, software, and manual procedures that create an overall control environment.

General controls include software controls, physical hardware controls, computer operations controls, data security controls, controls over implementation of system processes, and administrative controls. Table 8-3 describes the functions of each of these controls.

Application controls are specific controls unique to each computerized application, such as payroll or order processing. They include both automated and manual procedures that ensure that only authorized data are completely and accurately processed by that application. Application controls can be classified as (1) input controls, (2) processing controls, and (3) output controls.

Input controls check data for accuracy and completeness when they enter the system. There are specific input controls for input authorization, data conversion, data editing, and error handling. *Processing controls* establish that data are complete and accurate during updating. *Output controls* ensure that

TABLE 8-3 GENERAL CONTROLS

TYPE OF GENERAL CONTROL	DESCRIPTION
Software controls	Monitor the use of system software and prevent unauthorized access of software programs, system software, and computer programs.
Hardware controls	Ensure that computer hardware is physically secure, and check for equipment malfunction. Organizations that are critically dependent on their computers also must make provisions for backup or continued operation to maintain constant service.
Computer operations controls	Oversee the work of the computer department to ensure that programmed procedures are consistently and correctly applied to the storage and processing of data. They include controls over the setup of computer processing jobs and backup and recovery procedures for processing that ends abnormally.
Data security controls	Ensure that valuable business data files on either disk or tape are not subject to unauthorized access, change, or destruction while they are in use or in storage.
Implementation controls	Audit the systems development process at various points to ensure that the process is properly controlled and managed.
Administrative controls	Formalize standards, rules, procedures, and control disciplines to ensure that the organization's general and application controls are properly executed and enforced.

the results of computer processing are accurate, complete, and properly distributed. You can find more detail about application and general controls in our Learning Tracks.

RISK ASSESSMENT

Before your company commits resources to security and information systems controls, it must know which assets require protection and the extent to which these assets are vulnerable. A risk assessment helps answer these questions and determine the most cost-effective set of controls for protecting assets.

A **risk assessment** determines the level of risk to the firm if a specific activity or process is not properly controlled. Not all risks can be anticipated and measured, but most businesses will be able to acquire some understanding of the risks they face. Business managers working with information systems specialists should try to determine the value of information assets, points of vulnerability, the likely frequency of a problem, and the potential for damage. For example, if an event is likely to occur no more than once a year, with a maximum of a $1,000 loss to the organization, it is not be wise to spend $20,000 on the design and maintenance of a control to protect against that event. However, if that same event could occur at least once a day, with a potential loss of more than $300,000 a year, $100,000 spent on a control might be entirely appropriate.

Table 8-4 illustrates sample results of a risk assessment for an online order processing system that processes 30,000 orders per day. The likelihood of each exposure occurring over a one-year period is expressed as a percentage. The next column shows the highest and lowest possible loss that could be expected each time the exposure occurred and an average loss calculated by adding the highest and lowest figures together and dividing by two. The expected annual loss for each exposure can be determined by multiplying the average loss by its probability of occurrence.

This risk assessment shows that the probability of a power failure occurring in a one-year period is 30 percent. Loss of order transactions while power is down could range from $5,000 to $200,000 (averaging $102,500) for each occurrence, depending on how long processing is halted. The probability of embezzlement occurring over a yearly period is about 5 percent, with potential losses ranging from $1,000 to $50,000 (and averaging $25,500) for each occurrence. User errors have a 98 percent chance of occurring over a yearly period, with losses ranging from $200 to $40,000 (and averaging $20,100) for each occurrence.

Once the risks have been assessed, system builders will concentrate on the control points with the greatest vulnerability and potential for loss. In this case, controls should focus on ways to minimize the risk of power failures and user errors because anticipated annual losses are highest for these areas.

TABLE 8-4 ONLINE ORDER PROCESSING RISK ASSESSMENT

EXPOSURE	PROBABILITY OF OCCURRENCE (%)	LOSS RANGE/ AVERAGE ($)	EXPECTED ANNUAL LOSS ($)
Power failure	30%	$5,000–$200,000 ($102,500)	$30,750
Embezzlement	5%	$1,000–$50,000 ($25,500)	$1,275
User error	98%	$200–$40,000 ($20,100)	$19,698

SECURITY POLICY

Once you've identified the main risks to your systems, your company will need to develop a security policy for protecting the company's assets. A **security policy** consists of statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving these goals. What are the firm's most important information assets? Who generates and controls this information in the firm? What existing security policies are in place to protect the information? What level of risk is management willing to accept for each of these assets? Is it willing, for instance, to lose customer credit data once every 10 years? Or will it build a security system for credit card data that can withstand the once-in-a-hundred-year disaster? Management must estimate how much it will cost to achieve this level of acceptable risk.

The security policy drives policies determining acceptable use of the firm's information resources and which members of the company have access to its information assets. An **acceptable use policy (AUP)** defines acceptable uses of the firm's information resources and computing equipment, including desktop and laptop computers, wireless devices, telephones, and the Internet. The policy should clarify company policy regarding privacy, user responsibility, and personal use of company equipment and networks. A good AUP defines unacceptable and acceptable actions for every user and specifies consequences for noncompliance. For example, security policy at Unilever, the giant multinational consumer goods company, requires every employee equipped with a laptop or mobile handheld device to use a company-specified device and employ a password or other method of identification when logging onto the corporate network.

Security policy also includes provisions for identity management. **Identity management** consists of business processes and software tools for identifying the valid users of a system and controlling their access to system resources. It includes policies for identifying and authorizing different categories of system users, specifying what systems or portions of systems each user is allowed to access, and the processes and technologies for authenticating users and protecting their identities.

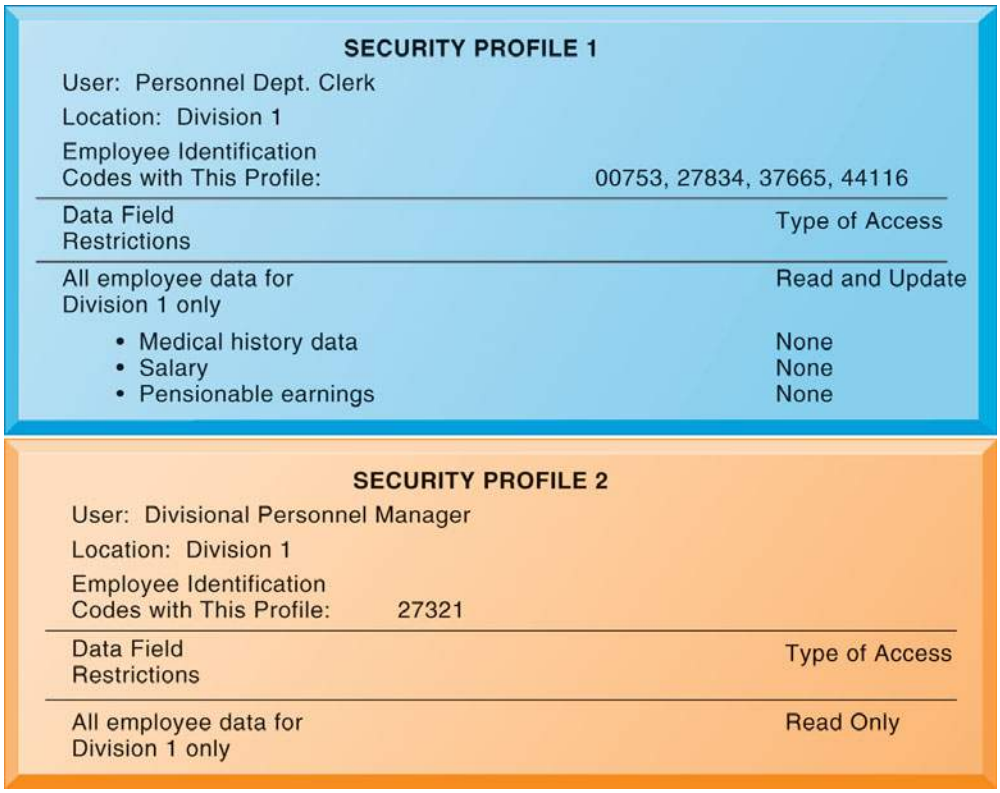
Figure 8-3 is one example of how an identity management system might capture the access rules for different levels of users in the human resources function. It specifies what portions of a human resource database each user is permitted to access, based on the information required to perform that person's job. The database contains sensitive personal information such as employees' salaries, benefits, and medical histories.

The access rules illustrated here are for two sets of users. One set of users consists of all employees who perform clerical functions, such as inputting employee data into the system. All individuals with this type of profile can update the system but can neither read nor update sensitive fields, such as salary, medical history, or earnings data. Another profile applies to a divisional manager, who cannot update the system but who can read all employee data fields for his or her division, including medical history and salary. We provide more detail on the technologies for user authentication later on in this chapter.

DISASTER RECOVERY PLANNING AND BUSINESS CONTINUITY PLANNING

If you run a business, you need to plan for events, such as power outages, floods, earthquakes, or terrorist attacks that will prevent your information systems and your business from operating. **Disaster recovery planning** devises

FIGURE 8-3 ACCESS RULES FOR A PERSONNEL SYSTEM



SECURITY PROFILE 1

User: Personnel Dept. Clerk

Location: Division 1

Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2

User: Divisional Personnel Manager

Location: Division 1

Employee Identification Codes with This Profile: 27321

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

These two examples represent two security profiles or data security patterns that might be found in a personnel system. Depending on the access rules, a user would have certain restrictions on access to various systems, locations, or data in an organization.

plans for the restoration of computing and communications services after they have been disrupted. Disaster recovery plans focus primarily on the technical issues involved in keeping systems up and running, such as which files to back up and the maintenance of backup computer systems or disaster recovery services.

For example, MasterCard maintains a duplicate computer center in Kansas City, Missouri, to serve as an emergency backup to its primary computer center in St. Louis. Rather than build their own backup facilities, many firms contract with disaster recovery firms, such as Comdisco Disaster Recovery Services in Rosemont, Illinois, and SunGard Availability Services, headquartered in Wayne, Pennsylvania. These disaster recovery firms provide hot sites housing spare computers at locations around the country where subscribing firms can run their critical applications in an emergency. For example, Champion Technologies, which supplies chemicals used in oil and gas operations, is able to switch its enterprise systems from Houston to a SunGard hot site in Scottsdale, Arizona, in two hours.

Business continuity planning focuses on how the company can restore business operations after a disaster strikes. The business continuity plan identifies critical business processes and determines action plans for handling mission-critical functions if systems go down. For example, Deutsche Bank, which provides investment banking and asset management services in 74 different countries, has a well-developed business continuity plan that it continually updates and refines. It maintains full-time teams in Singapore, Hong Kong, Japan, India, and Australia

to coordinate plans addressing loss of facilities, personnel, or critical systems so that the company can continue to operate when a catastrophic event occurs. Deutsche Bank's plan distinguishes between processes critical for business survival and those critical to crisis support and is coordinated with the company's disaster recovery planning for its computer centers.

Business managers and information technology specialists need to work together on both types of plans to determine which systems and business processes are most critical to the company. They must conduct a business impact analysis to identify the firm's most critical systems and the impact a systems outage would have on the business. Management must determine the maximum amount of time the business can survive with its systems down and which parts of the business must be restored first.

THE ROLE OF AUDITING

How does management know that information systems security and controls are effective? To answer this question, organizations must conduct comprehensive and systematic audits. An **MIS audit** examines the firm's overall security environment as well as controls governing individual information systems. The auditor should trace the flow of sample transactions through the system and perform tests, using, if appropriate, automated audit software. The MIS audit may also examine data quality.

Security audits review technologies, procedures, documentation, training, and personnel. A thorough audit will even simulate an attack or disaster to test the response of the technology, information systems staff, and business employees.

The audit lists and ranks all control weaknesses and estimates the probability of their occurrence. It then assesses the financial and organizational impact of each threat. Figure 8-4 is a sample auditor's listing of control weaknesses for a loan system. It includes a section for notifying management of such weaknesses and for management's response. Management is expected to devise a plan for countering significant weaknesses in controls.

8.4 Technologies and Tools for Protecting Information Resources

Businesses have an array of technologies for protecting their information resources. They include tools for managing user identities, preventing unauthorized access to systems and data, ensuring system availability, and ensuring software quality.

IDENTITY MANAGEMENT AND AUTHENTICATION

Large and midsize companies have complex IT infrastructures and many different systems, each with its own set of users. Identity management software automates the process of keeping track of all these users and their system privileges, assigning each user a unique digital identity for accessing each system. It also includes tools for authenticating users, protecting user identities, and controlling access to system resources.

To gain access to a system, a user must be authorized and authenticated. **Authentication** refers to the ability to know that a person is who he or she

FIGURE 8-4 SAMPLE AUDITOR'S LIST OF CONTROL WEAKNESSES

Function: Loans **Location: Peoria, IL**	**Prepared by: J. Ericson** **Date: June 16, 2011**		**Received by: T. Benson** **Review date: June 28, 2011**	
Nature of Weakness and Impact	Chance for Error/Abuse		Notification to Management	
	Yes/ No	Justification	Report date	Management response
User accounts with missing passwords	Yes	Leaves system open to unauthorized outsiders or attackers	5/10/11	Eliminate accounts without passwords
Network configured to allow some sharing of system files	Yes	Exposes critical system files to hostile parties connected to the network	5/10/11	Ensure only required directories are shared and that they are protected with strong passwords
Software patches can update production programs without final approval from Standards and Controls group	No	All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status		

This chart is a sample page from a list of control weaknesses that an auditor might find in a loan system in a local commercial bank. This form helps auditors record and evaluate control weaknesses and shows the results of discussing those weaknesses with management, as well as any corrective actions taken by management.

claims to be. Authentication is often established by using **passwords** known only to authorized users. An end user uses a password to log on to a computer system and may also use passwords for accessing specific systems and files. However, users often forget passwords, share them, or choose poor passwords that are easy to guess, which compromises security. Password systems that are too rigorous hinder employee productivity. When employees must change complex passwords frequently, they often take shortcuts, such as choosing passwords that are easy to guess or writing down their passwords at their workstations in plain view. Passwords can also be "sniffed" if transmitted over a network or stolen through social engineering.

New authentication technologies, such as tokens, smart cards, and biometric authentication, overcome some of these problems. A **token** is a physical device, similar to an identification card, that is designed to prove the identity of a single user. Tokens are small gadgets that typically fit on key rings and display passcodes that change frequently. A **smart card** is a device about the size of a credit card that contains a chip formatted with access permission and other data. (Smart cards are also used in electronic payment systems.) A reader device interprets the data on the smart card and allows or denies access.

Biometric authentication uses systems that read and interpret individual human traits, such as fingerprints, irises, and voices, in order to grant or deny access. Biometric authentication is based on the measurement of a physical or behavioral trait that makes each individual unique. It compares a person's unique characteristics, such as the fingerprints, face, or retinal image, against a

This PC has a biometric fingerprint reader for fast yet secure access to files and networks. New models of PCs are starting to use biometric identification to authenticate users.

stored profile of these characteristics to determine whether there are any differences between these characteristics and the stored profile. If the two profiles match, access is granted. Fingerprint and facial recognition technologies are just beginning to be used for security applications, with many PC laptops equipped with fingerprint identification devices and several models with built-in webcams and face recognition software.

FIREWALLS, INTRUSION DETECTION SYSTEMS, AND ANTIVIRUS SOFTWARE

Without protection against malware and intruders, connecting to the Internet would be very dangerous. Firewalls, intrusion detection systems, and antivirus software have become essential business tools.

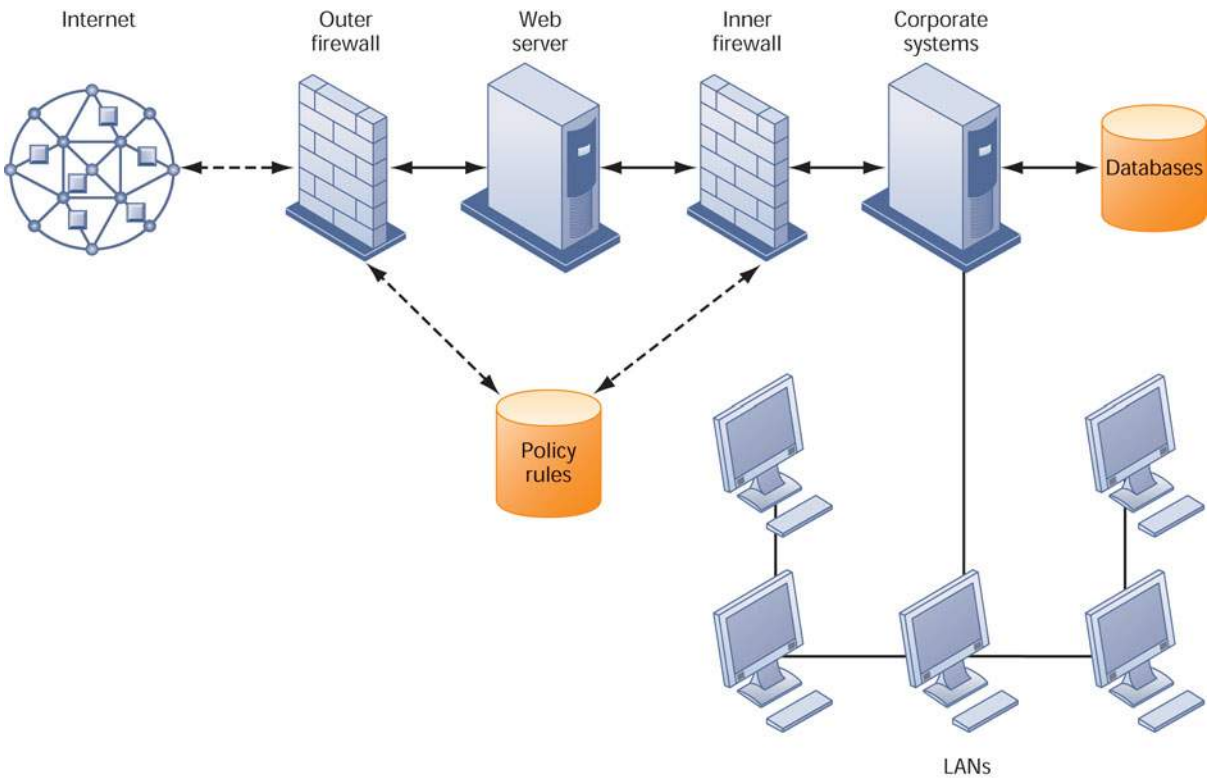
Firewalls

Firewalls prevent unauthorized users from accessing private networks. A firewall is a combination of hardware and software that controls the flow of incoming and outgoing network traffic. It is generally placed between the organization's private internal networks and distrusted external networks, such as the Internet, although firewalls can also be used to protect one part of a company's network from the rest of the network (see Figure 8-5).

The firewall acts like a gatekeeper who examines each user's credentials before access is granted to a network. The firewall identifies names, IP addresses, applications, and other characteristics of incoming traffic. It checks this information against the access rules that have been programmed into the system by the network administrator. The firewall prevents unauthorized communication into and out of the network.

In large organizations, the firewall often resides on a specially designated computer separate from the rest of the network, so no incoming request directly accesses private network resources. There are a number of firewall screening technologies, including static packet filtering, stateful inspection, Network Address Translation, and application proxy filtering. They are frequently used in combination to provide firewall protection.

FIGURE 8-5 A CORPORATE FIREWALL



The firewall is placed between the firm's private network and the public Internet or another distrusted network to protect against unauthorized traffic.

Packet filtering examines selected fields in the headers of data packets flowing back and forth between the trusted network and the Internet, examining individual packets in isolation. This filtering technology can miss many types of attacks. *Stateful inspection* provides additional security by determining whether packets are part of an ongoing dialogue between a sender and a receiver. It sets up state tables to track information over multiple packets. Packets are accepted or rejected based on whether they are part of an approved conversation or whether they are attempting to establish a legitimate connection.

Network Address Translation (NAT) can provide another layer of protection when static packet filtering and stateful inspection are employed. NAT conceals the IP addresses of the organization's internal host computer(s) to prevent sniffer programs outside the firewall from ascertaining them and using that information to penetrate internal systems.

Application proxy filtering examines the application content of packets. A proxy server stops data packets originating outside the organization, inspects them, and passes a proxy to the other side of the firewall. If a user outside the company wants to communicate with a user inside the organization, the outside user first "talks" to the proxy application and the proxy application communicates with the firm's internal computer. Likewise, a computer user inside the organization goes through the proxy to talk with computers on the outside.

To create a good firewall, an administrator must maintain detailed internal rules identifying the people, applications, or addresses that are allowed or rejected. Firewalls can deter, but not completely prevent, network penetration by outsiders and should be viewed as one element in an overall security plan.

Intrusion Detection Systems

In addition to firewalls, commercial security vendors now provide intrusion detection tools and services to protect against suspicious network traffic and attempts to access files and databases. **Intrusion detection systems** feature full-time monitoring tools placed at the most vulnerable points or "hot spots" of corporate networks to detect and deter intruders continually. The system generates an alarm if it finds a suspicious or anomalous event. Scanning software looks for patterns indicative of known methods of computer attacks, such as bad passwords, checks to see if important files have been removed or modified, and sends warnings of vandalism or system administration errors. Monitoring software examines events as they are happening to discover security attacks in progress. The intrusion detection tool can also be customized to shut down a particularly sensitive part of a network if it receives unauthorized traffic.

Antivirus and Antispyware Software

Defensive technology plans for both individuals and businesses must include antivirus protection for every computer. **Antivirus software** is designed to check computer systems and drives for the presence of computer viruses. Often the software eliminates the virus from the infected area. However, most antivirus software is effective only against viruses already known when the software was written. To remain effective, the antivirus software must be continually updated. Antivirus products are available for many different types of mobile and handheld devices in addition to servers, workstations, and desktop PCs.

Leading antivirus software vendors, such as McAfee, Symantec, and Trend Micro, have enhanced their products to include protection against spyware. Antispyware software tools such as Ad-Aware, Spybot S&D, and Spyware Doctor are also very helpful.

Unified Threat Management Systems

To help businesses reduce costs and improve manageability, security vendors have combined into a single appliance various security tools, including firewalls, virtual private networks, intrusion detection systems, and Web content filtering and antispam software. These comprehensive security management products are called **unified threat management (UTM)** systems. Although initially aimed at small and medium-sized businesss, UTM products are available for all sizes of networks. Leading UTM vendors include Crossbeam, Fortinent, and Check Point, and networking vendors such as Cisco Systems and Juniper Networks provide some UTM capabilities in their equipment.

SECURING WIRELESS NETWORKS

Despite its flaws, WEP provides some margin of security if Wi-Fi users remember to activate it. A simple first step to thwart hackers is to assign a unique name to your network's SSID and instruct your router not to broadcast it. Corporations can further improve Wi-Fi security by using it in conjunction with virtual private network (VPN) technology when accessing internal corporate data.

In June 2004, the Wi-Fi Alliance industry trade group finalized the 802.11i specification (also referred to as Wi-Fi Protected Access 2 or WPA2) that replaces WEP with stronger security standards. Instead of the static encryption keys used in WEP, the new standard uses much longer keys that continually change, making them harder to crack. It also employs an encrypted authentica-

tion system with a central authentication server to ensure that only authorized users access the network.

ENCRYPTION AND PUBLIC KEY INFRASTRUCTURE

Many businesses use encryption to protect digital information that they store, physically transfer, or send over the Internet. **Encryption** is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the intended receiver. Data are encrypted by using a secret numerical code, called an encryption key, that transforms plain data into cipher text. The message must be decrypted by the receiver.

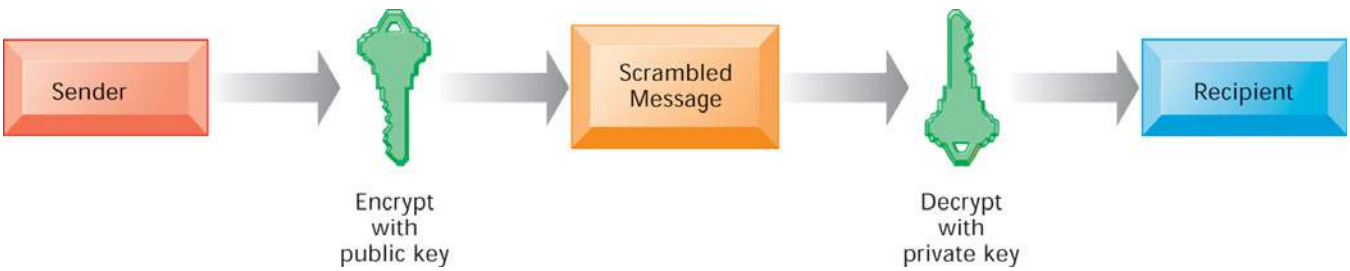
Two methods for encrypting network traffic on the Web are SSL and S-HTTP. **Secure Sockets Layer (SSL)** and its successor Transport Layer Security (TLS) enable client and server computers to manage encryption and decryption activities as they communicate with each other during a secure Web session. **Secure Hypertext Transfer Protocol (S-HTTP)** is another protocol used for encrypting data flowing over the Internet, but it is limited to individual messages, whereas SSL and TLS are designed to establish a secure connection between two computers.

The capability to generate secure sessions is built into Internet client browser software and servers. The client and the server negotiate what key and what level of security to use. Once a secure session is established between the client and the server, all messages in that session are encrypted.

There are two alternative methods of encryption: symmetric key encryption and public key encryption. In symmetric key encryption, the sender and receiver establish a secure Internet session by creating a single encryption key and sending it to the receiver so both the sender and receiver share the same key. The strength of the encryption key is measured by its bit length. Today, a typical key will be 128 bits long (a string of 128 binary digits).

The problem with all symmetric encryption schemes is that the key itself must be shared somehow among the senders and receivers, which exposes the key to outsiders who might just be able to intercept and decrypt the key. A more secure form of encryption called **public key encryption** uses two keys: one shared (or public) and one totally private as shown in Figure 8-6. The keys are mathematically related so that data encrypted with one key can be decrypted using only the other key. To send and receive messages, communi-

FIGURE 8-6 PUBLIC KEY ENCRYPTION



A public key encryption system can be viewed as a series of public and private keys that lock data when they are transmitted and unlock the data when they are received. The sender locates the recipient's public key in a directory and uses it to encrypt a message. The message is sent in encrypted form over the Internet or a private network. When the encrypted message arrives, the recipient uses his or her private key to decrypt the data and read the message.

cators first create separate pairs of private and public keys. The public key is kept in a directory and the private key must be kept secret. The sender encrypts a message with the recipient's public key. On receiving the message, the recipient uses his or her private key to decrypt it.

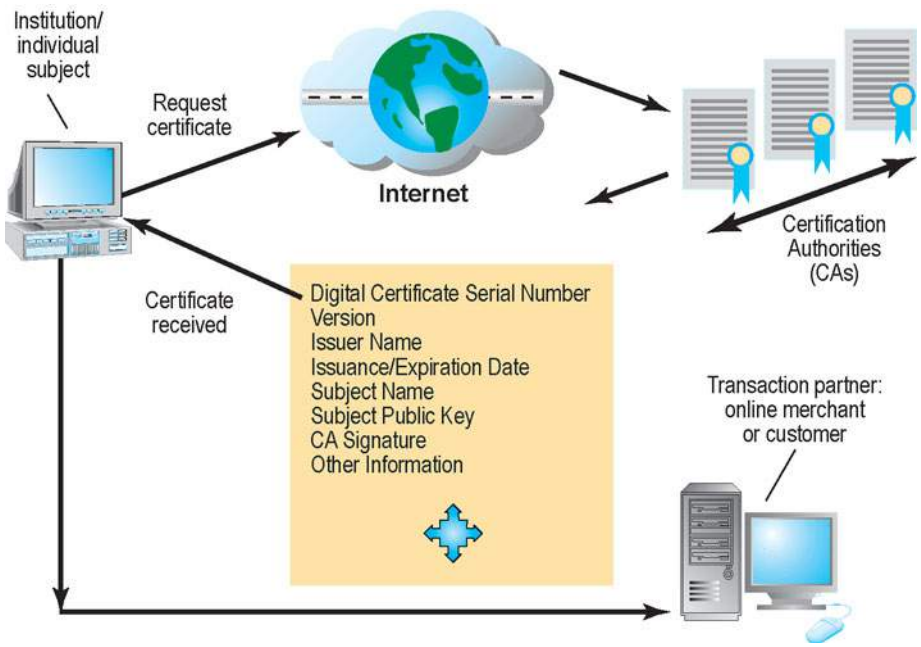
Digital certificates are data files used to establish the identity of users and electronic assets for protection of online transactions (see Figure 8-7). A digital certificate system uses a trusted third party, known as a certificate authority (CA, or certification authority), to validate a user's identity. There are many CAs in the United States and around the world, including VeriSign, IdenTrust, and Australia's KeyPost.

The CA verifies a digital certificate user's identity offline. This information is put into a CA server, which generates an encrypted digital certificate containing owner identification information and a copy of the owner's public key. The certificate authenticates that the public key belongs to the designated owner. The CA makes its own public key available publicly either in print or perhaps on the Internet. The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it was issued by the CA, and then obtains the sender's public key and identification information contained in the certificate. Using this information, the recipient can send an encrypted reply. The digital certificate system would enable, for example, a credit card user and a merchant to validate that their digital certificates were issued by an authorized and trusted third party before they exchange data. **Public key infrastructure (PKI)**, the use of public key cryptography working with a CA, is now widely used in e-commerce.

ENSURING SYSTEM AVAILABILITY

As companies increasingly rely on digital networks for revenue and operations, they need to take additional steps to ensure that their systems and applications

FIGURE 8-7 DIGITAL CERTIFICATES



Digital certificates help establish the identity of people or electronic assets. They protect online transactions by providing secure, encrypted, online communication.

are always available. Firms such as those in the airline and financial services industries with critical applications requiring online transaction processing have traditionally used fault-tolerant computer systems for many years to ensure 100-percent availability. In **online transaction processing**, transactions entered online are immediately processed by the computer. Multitudinous changes to databases, reporting, and requests for information occur each instant.

Fault-tolerant computer systems contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service. Fault-tolerant computers use special software routines or self-checking logic built into their circuitry to detect hardware failures and automatically switch to a backup device. Parts from these computers can be removed and repaired without disruption to the computer system.

Fault tolerance should be distinguished from **high-availability computing**. Both fault tolerance and high-availability computing try to minimize downtime. **Downtime** refers to periods of time in which a system is not operational. However, high-availability computing helps firms recover quickly from a system crash, whereas fault tolerance promises continuous availability and the elimination of recovery time altogether.

High-availability computing environments are a minimum requirement for firms with heavy e-commerce processing or for firms that depend on digital networks for their internal operations. High-availability computing requires backup servers, distribution of processing across multiple servers, high-capacity storage, and good disaster recovery and business continuity plans. The firm's computing platform must be extremely robust with scalable processing power, storage, and bandwidth.

Researchers are exploring ways to make computing systems recover even more rapidly when mishaps occur, an approach called **recovery-oriented computing**. This work includes designing systems that recover quickly, and implementing capabilities and tools to help operators pinpoint the sources of faults in multi-component systems and easily correct their mistakes.

Controlling Network Traffic: Deep Packet Inspection

Have you ever tried to use your campus network and found it was very slow? It may be because your fellow students are using the network to download music or watch YouTube. Bandwith-consuming applications such as file-sharing programs, Internet phone service, and online video are able to clog and slow down corporate networks, degrading performance. For example, Ball Sate University in Muncie, Indiana, found its network had slowed because a small minority of students were using peer-to-peer file-sharing programs to download movies and music.

A technology called **deep packet inspection (DPI)** helps solve this problem. DPI examines data files and sorts out low-priority online material while assigning higher priority to business-critical files. Based on the priorities established by a network's operators, it decides whether a specific data packet can continue to its destination or should be blocked or delayed while more important traffic proceeds. Using a DPI system from Allot Communications, Ball State was able to cap the amount of file-sharing traffic and assign it a much lower priority. Ball State's preferred network traffic speeded up.

Security Outsourcing

Many companies, especially small businesses, lack the resources or expertise to provide a secure high-availability computing environment on their own. They can outsource many security functions to **managed security service**

providers (MSSPs) that monitor network activity and perform vulnerability testing and intrusion detection. SecureWorks, BT Managed Security Solutions Group, and Symantec are leading providers of MSSP services.

SECURITY ISSUES FOR CLOUD COMPUTING AND THE MOBILE DIGITAL PLATFORM

Although cloud computing and the emerging mobile digital platform have the potential to deliver powerful benefits, they pose new challenges to system security and reliability. We now describe some of these challenges and how they should be addressed.

Security in the Cloud

When processing takes place in the cloud, accountability and responsibility for protection of sensitive data still reside with the company owning that data. Understanding how the cloud computing provider organizes its services and manages the data is critical. The Interactive Session on Technology details some of the cloud security issues that should be addressed.

Cloud users need to confirm that regardless of where their data are stored or transferred, they are protected at a level that meets their corporate requirements. They should stipulate that the cloud provider store and process data in specific jurisdictions according to the privacy rules of those jurisdictions. Cloud clients should find how the cloud provider segregates their corporate data from those of other companies and ask for proof that encryption mechanisms are sound. It's also important to know how the cloud provider will respond if a disaster strikes, whether the provider will be able to completely restore your data, and how long this should take. Cloud users should also ask whether cloud providers will submit to external audits and security certifications. These kinds of controls can be written into the service level agreement (SLA) before to signing with a cloud provider.

Securing Mobile Platforms

If mobile devices are performing many of the functions of computers, they need to be secured like desktops and laptops against malware, theft, accidental loss, unauthorized access, and hacking attempts. Mobile devices accessing corporate systems and data require special protection.

Companies should make sure that their corporate security policy includes mobile devices, with additional details on how mobile devices should be supported, protected, and used. They will need tools to authorize all devices in use; to maintain accurate inventory records on all mobile devices, users, and applications; to control updates to applications; and to lock down lost devices so they can't be compromised. Firms should develop guidelines stipulating approved mobile platforms and software applications as well as the required software and procedures for remote access of corporate systems. Companies will need to ensure that all smartphones are up to date with the latest security patches and antivirus/antispam software, and they should encrypt communication whenever possible.

ENSURING SOFTWARE QUALITY

In addition to implementing effective security and controls, organizations can improve system quality and reliability by employing software metrics and rigorous software testing. Software metrics are objective assessments of the system in the form of quantified measurements. Ongoing use of metrics allows

INTERACTIVE SESSION: TECHNOLOGY

HOW SECURE IS THE CLOUD?

New York-based investment banking and financial services firm Cowen and Co. has moved its global sales systems to the cloud using Salesforce.com. So far, Cowen's CIO Daniel Flax is pleased. Using cloud services has helped the company lower upfront technology costs, decrease downtime and support additional services. But he's trying to come to grips with cloud security issues.Cloud computing is indeed cloudy, and this lack of transparency is troubling to many.

One of the biggest risks of cloud computing is that it is highly distributed. Cloud applications and application mash-ups reside in virtual libraries in large remote data centers and server farms that supply business services and data management for multiple corporate clients. To save money and keep costs low, cloud computing providers often distribute work to data centers around the globe where work can be accomplished most efficiently. When you use the cloud, you may not know precisely where your data are being hosted, and you might not even know the country where they are being stored.

The dispersed nature of cloud computing makes it difficult to track unauthorized activity. Virtually all cloud providers use encryption, such as Secure Sockets Layer, to secure the data they handle while the data are being transmitted. But if the data are stored on devices that also store other companies' data, it's important to ensure these stored data are encrypted as well.

Indian Harvest Specialtifoods, a Bemidji, Minnesota-based company that distributes rice, grains, and legumes to restaurants worldwide, relies on cloud software provider NetSuite to ensure that its data sent to the cloud are fully protected. Mike Mullin, Indian Harvest's IT director, feels that using SSL (Secure Sockets Layer) to encrypt the data gives him some level of confidence that the data are secure. He also points out that his company and other users of cloud services need to pay attention to their own security practices, especially access controls. "Your side of the infrastructure is just as vulnerable, if not more vulnerable, than the provider's side," he observes.

One way to deal with these problems is to use a cloud vendor that is a public company, which is required by law to disclose how it manages information. Salesforce.com meets this requirement, with strict processes and guidelines for managing its data centers. "We know our data are in the U.S. and we have a report on the very data centers that we're talking about, " says Flax.

Another alternative is to use a cloud provider that give subscribers the option to choose where their cloud computing work takes place. For example, Terremark Worldwide Inc. is giving its subscriber Agora Games the option to choose where its applications run. Terremark has a Miami facility but is adding other locations. In the past, Agora had no say over where Terremark hosted its applications and data.

Even if your data are totally secure in the cloud, you may not be able to prove it. Some cloud providers don't meet current compliance requirements regarding security, and some of those providers, such as Amazon, have asserted that they don't intend to meet those rules and won't allow compliance auditors on-site.

There are laws restricting where companies can send and store some types of information—personally identifiable information in the European Union (EU), government work in the United Sates or applications that employ certain encryption algorithms. Companies required to meet these regulations involving protected data either in the United States or the EU won't be able to use public cloud providers.

Some of these regulations call for proof that systems are securely managed, which may require confirmation from an independent audit. Large providers are unlikely to allow another company's auditors to inspect their data centers. Microsoft found a way to deal with this problem that may be helpful. The company reduced 26 different types of audits to a list of 200 necessary controls for meeting compliance standards that were applied to its data center environments and services. Microsoft does not give every customer or auditor access to its data centers, but its compliance framework allows auditors to order from a menu of tests and receive the results.

Companies expect their systems to be running 24/7, but cloud providers haven't always been able to provide this level of service. Millions of customers of Salesforce.com suffered a 38-minute outage in early January 2009 and others several years earlier. The January 2009 outage locked more than 900,000 subscribers out of crucial applications and data

needed to transact business with customers. More than 300,000 customers using Intuit's online network of small business aplications were unable to access these services for two days in June 2010 following a power outage.

Agreements for services such as Amazon EC2 and Microsoft Azure state that these companies are not going to be held liable for data losses or fines or other legal penalties when companies use their services. Both vendors offer guidance on how to use their cloud platforms securely, and they may still be able to protect data better than some companies' home-grown facilities.

Salesforce.com had been building up and redesigning its infrastructure to ensure better service. The company invested $50 million in Mirrorforce technology, a mirroring system that creates a duplicate database in a separate location and synchronizes the data instantaneously. If one database is disabled, the other takes over. Salesforce.com added two data centers on the East and West coasts in addition to its Silicon Valley facility. The company distributed processing for its larger customers among these centers to balance its database load.

Sources: Seth Fineberg, "A Shadow on the Cloud?" *Information Management*, August, 2010; Ellen Messmer, "Secrecy of Cloud Computing Providers Raises IT Security Risks," *IT World*, July 13, 2010; John Edwards, "Cutting Through the Fog of Cloud Security," *Computerworld*, February 23, 2009; Wayne Rash, "Is Cloud Computing Secure? Prove It," *eWeek*, September 21, 2009; Robert Lemos, "Five Lessons from Microsoft on Cloud Security," *Computerworld*, August 25, 2009; and Mike Fratto, "Cloud Control," *Information Week*, January 26, 2009.

CASE STUDY QUESTIONS

1. What security and control problems are described in this case?
2. What people, organization, and technology factors contribute to these problems?
3. How secure is cloud computing? Explain your answer.
4. If you were in charge of your company's information systems department, what issues would you want to clarify with prospective vendors?
5. Would you entrust your corporate systems to a cloud computing provider? Why or why not?

MIS IN ACTION

Go to www.trust.salesforce.com, then answer the following questions:

1. Click on Security and describe Salesforce.com's security provisions. How helpful are these?
2. Click on Best Practices and describe what subscribing companies can do to tighten security. How helpful are these guidelines?
3. If you ran a business, would you feel confident about using Salesforce.com's on-demand service? Why or why not?

the information systems department and end users to jointly measure the performance of the system and identify problems as they occur. Examples of software metrics include the number of transactions that can be processed in a specified unit of time, online response time, the number of payroll checks printed per hour, and the number of known bugs per hundred lines of program code. For metrics to be successful, they must be carefully designed, formal, objective, and used consistently.

Early, regular, and thorough testing will contribute significantly to system quality. Many view testing as a way to prove the correctness of work they have done. In fact, we know that all sizable software is riddled with errors, and we must test to uncover these errors.

Good testing begins before a software program is even written by using a *walkthrough*—a review of a specification or design document by a small group of people carefully selected based on the skills needed for the particular objectives being tested. Once developers start writing software programs, coding walkthroughs also can be used to review program code. However, code must

be tested by computer runs. When errors are discovered, the source is found and eliminated through a process called *debugging*. You can find out more about the various stages of testing required to put an information system into operation in Chapter 13. Our Learning Tracks also contain descriptions of methodologies for developing software programs that also contribute to software quality.

8.5 Hands-on MIS Projects

The projects in this section give you hands-on experience analyzing security vulnerabilities, using spreadsheet software for risk analysis, and using Web tools to research security outsourcing services.

Management Decision Problems

1. K2 Network operates online game sites used by about 16 million people in over 100 countries. Players are allowed to enter a game for free, but must buy digital "assets" from K2, such as swords to fight dragons, if they want to be deeply involved. The games can accommodate millions of players at once and are played simultaneously by people all over the world. Prepare a security analysis for this Internet-based business. What kinds of threats should it anticipate? What would be their impact on the business? What steps can it take to prevent damage to its Web sites and continuing operations?
2. A survey of your firm's information technology infrastructure has produced the following security analysis statistics:

SECURITY VULNERABILITIES BY TYPE OF COMPUTING PLATFORM

PLATFORM	NUMBER OF COMPUTERS	HIGH RISK	MEDIUM RISK	LOW RISK	TOTAL VULNERABILITIES
Windows Server (corporate applications)	1	11	37	19	
Windows 7 Enterprise (high-level administrators)	3	56	242	87	
Linux (e-mail and printing services)	1	3	154	98	
Sun Solaris (Unix) (E-commerce and Web servers)	2	12	299	78	
Windows 7 Enterprise user desktops and laptops with office productivity tools that can also be linked to the corporate network running corporate applications and intranet	195	14	16	1,237	

High risk vulnerabilities include non-authorized users accessing applications, guessable passwords, user names matching the password, active user accounts with missing passwords, and the existence of unauthorized programs in application systems.

Medium risk vulnerabilities include the ability of users to shut down the system without being logged on, passwords and screen saver settings that were

not established for PCs, and outdated versions of software still being stored on hard drives.

Low risk vulnerabilities include the inability of users to change their passwords, user passwords that have not been changed periodically, and passwords that were smaller than the minimum size specified by the company.

- Calculate the total number of vulnerabilities for each platform. What is the potential impact of the security problems for each computing platform on the organization?
- If you only have one information systems specialist in charge of security, which platforms should you address first in trying to eliminate these vulnerabilities? Second? Third? Last? Why?
- Identify the types of control problems illustrated by these vulnerabilities and explain the measures that should be taken to solve them.
- What does your firm risk by ignoring the security vulnerabilities identified?

Improving Decision Making: Using Spreadsheet Software to Perform a Security Risk Assessment

Software skills: Spreadsheet formulas and charts
Business skills: Risk assessment

This project uses spreadsheet software to calculate anticipated annual losses from various security threats identified for a small company.

Mercer Paints is a small but highly regarded paint manufacturing company located in Alabama. The company has a network in place linking many of its business operations. Although the firm believes that its security is adequate, the recent addition of a Web site has become an open invitation to hackers. Management requested a risk assessment. The risk assessment identified a number of potential exposures. These exposures, their associated probabilities, and average losses are summarized in the following table.

MERCER PAINTS RISK ASSESSMENT

EXPOSURE	PROBABILITY OF OCCURRENCE	AVERAGE LOSS
Malware attack	60%	$75,000
Data loss	12%	$70,000
Embezzlement	3%	$30,000
User errors	95%	$25,000
Threats from hackers	95%	$90,000
Improper use by employees	5%	$5,000
Power failure	15%	$300,000

- In addition to the potential exposures listed, you should identify at least three other potential threats to Mercer Paints, assign probabilities, and estimate a loss range.
- Use spreadsheet software and the risk assessment data to calculate the expected annual loss for each exposure.
- Present your findings in the form of a chart. Which control points have the greatest vulnerability? What recommendations would you make to Mercer Paints? Prepare a written report that summarizes your findings and recommendations.

Improving Decision Making: Evaluating Security Outsourcing Services

Software skills: Web browser and presentation software
Business skills: Evaluating business outsourcing services

Businesses today have a choice of whether to outsource the security function or maintain their own internal staff for this purpose. This project will help develop your Internet skills in using the Web to research and evaluate security outsourcing services.

As an information systems expert in your firm, you have been asked to help management decide whether to outsource security or keep the security function within the firm. Search the Web to find information to help you decide whether to outsource security and to locate security outsourcing services.

- Present a brief summary of the arguments for and against outsourcing computer security for your company.
- Select two firms that offer computer security outsourcing services, and compare them and their services.
- Prepare an electronic presentation for management summarizing your findings. Your presentation should make the case on whether or not your company should outsource computer security. If you believe your company should outsource, the presentation should identify which security outsourcing service should be selected and justify your selection.

Learning Track Modules

The following Learning Tracks provide content relevant to topics covered in this chapter:

1. The Booming Job Market in IT Security
2. The Sarbanes-Oxley Act
3. Computer Forensics
4. General and Application Controls for Information Systems
5. Management Challenges of Security and Control
6. Software Vulnerability and Reliability

Review Summary

1. *Why are information systems vulnerable to destruction, error, and abuse?*

   Digital data are vulnerable to destruction, misuse, error, fraud, and hardware or software failures. The Internet is designed to be an open system and makes internal corporate systems more vulnerable to actions from outsiders. Hackers can unleash denial-of-service (DoS) attacks or penetrate corporate networks, causing serious system disruptions. Wi-Fi networks can easily be penetrated by intruders using sniffer programs to obtain an address to access the resources of the network. Computer viruses and worms can disable systems and Web sites. The dispersed nature of cloud computing makes it difficult to track unauthorized activity or to apply controls from afar. Software presents problems because software bugs may be impossible to eliminate and because software vulnerabilities can be exploited by hackers and malicious software. End users often introduce errors.

2. *What is the business value of security and control?*

   Lack of sound security and control can cause firms relying on computer systems for their core business functions to lose sales and productivity. Information assets, such as confidential employee records, trade secrets, or business plans, lose much of their value if they are revealed to outsiders or if they expose the firm to legal liability. New laws, such as HIPAA, the Sarbanes-Oxley Act, and the Gramm-Leach-Bliley Act, require companies to practice stringent electronic records management and adhere to strict standards for security, privacy, and control. Legal actions requiring electronic evidence and computer forensics also require firms to pay more attention to security and electronic records management.

3. *What are the components of an organizational framework for security and control?*

   Firms need to establish a good set of both general and application controls for their information systems. A risk assessment evaluates information assets, identifies control points and control weaknesses, and determines the most cost-effective set of controls. Firms must also develop a coherent corporate security policy and plans for continuing business operations in the event of disaster or disruption. The security policy includes policies for acceptable use and identity management. Comprehensive and systematic MIS auditing helps organizations determine the effectiveness of security and controls for their information systems.

4. *What are the most important tools and technologies for safeguarding information resources?*

   Firewalls prevent unauthorized users from accessing a private network when it is linked to the Internet. Intrusion detection systems monitor private networks from suspicious network traffic and attempts to access corporate systems. Passwords, tokens, smart cards, and biometric authentication are used to authenticate system users. Antivirus software checks computer systems for infections by viruses and worms and often eliminates the malicious software, while antispyware software combats intrusive and harmful spyware programs. Encryption, the coding and scrambling of messages, is a widely used technology for securing electronic transmissions over unprotected networks. Digital certificates combined with public key encryption provide further protection of electronic transactions by authenticating a user's identity. Companies can use fault-tolerant computer systems or create high-availability computing environments to make sure that their information systems are always available. Use of software metrics and rigorous software testing help improve software quality and reliability.

Key Terms

Acceptable use policy (AUP), 310
Antivirus software, 316
Application controls, 308
Authentication, 312
Biometric authentication, 313
Botnet, 299
Bugs, 303
Business continuity planning, 311
Click fraud, 302
Computer crime, 300
Computer forensics, 307
Computer virus, 296
Controls, 293
Cybervandalism, 298
Deep packet inspection (DPI), 319
Denial-of-service (DoS) attack, 299

Digital certificates, 318
Disaster recovery planning, 310
Distributed denial-of-service (DDoS) attack, 299
Downtime, 319
Encryption, 317
Evil twin, 301
Fault-tolerant computer systems, 319
Firewall, 314
General controls, 308
Gramm-Leach-Bliley Act, 306
Hacker, 298
High-availability computing, 319
HIPAA, 306
Identity management, 310
Identity theft, 301
Intrusion detection systems, 316
Keyloggers, 298
Malware, 296
Managed security service providers (MSSPs), 319
MIS audit, 312
Online transaction processing, 319
Password, 313
Patches, 303
Pharming, 301
Phishing, 301
Public key encryption, 317
Public key infrastructure (PKI), 318
Recovery-oriented computing, 319
Risk assessment, 309
Sarbanes-Oxley Act, 306
Secure Hypertext Transfer Protocol (S-HTTP), 317
Secure Sockets Layer (SSL), 317
Security, 293
Security policy, 310
SQL injection attack, 298
Smart card, 313
Sniffer, 299
Social engineering, 302
Spoofing, 299
Spyware, 298
Token, 313
Trojan horse, 298
Unified threat management (UTM), 316
War driving, 295
Worms, 296

Review Questions

1. Why are information systems vulnerable to destruction, error, and abuse?
- List and describe the most common threats against contemporary information systems.
- Define malware and distinguish among a virus, a worm, and a Trojan horse.
- Define a hacker and explain how hackers create security problems and damage systems.
- Define computer crime. Provide two examples of crime in which computers are targets and two examples in which computers are used as instruments of crime.
- Define identity theft and phishing and explain why identity theft is such a big problem today.
- Describe the security and system reliability problems created by employees.
- Explain how software defects affect system reliability and security.

2. What is the business value of security and control?
- Explain how security and control provide value for businesses.
- Describe the relationship between security and control and recent U.S. government regulatory requirements and computer forensics.

3. What are the components of an organizational framework for security and control?
- Define general controls and describe each type of general control.
- Define application controls and describe each type of application control.
- Describe the function of risk assessment and explain how it is conducted for information systems.
- Define and describe the following: security policy, acceptable use policy, and identity management.
- Explain how MIS auditing promotes security and control.

4. What are the most important tools and technologies for safeguarding information resources?
- Name and describe three authentication methods.
- Describe the roles of firewalls, intrusion detection systems, and antivirus software in promoting security.

- Explain how encryption protects information.
- Describe the role of encryption and digital certificates in a public key infrastructure.
- Distinguish between fault-tolerant and high-availability computing, and between disaster recovery planning and business continuity planning.
- Identify and describe the security problems posed by cloud computing.
- Describe measures for improving software quality and reliability.

Discussion Questions

1. Security isn't simply a technology issue, it's a business issue. Discuss.
2. If you were developing a business continuity plan for your company, where would you start? What aspects of the business would the plan address?
3. Suppose your business had an e-commerce Web site where it sold goods and accepted credit card payments. Discuss the major security threats to this Web site and their potential impact. What can be done to minimize these threats?

Video Cases

Video Cases and Instructional Videos illustrating some of the concepts in this chapter are available. Contact your instructor to access these videos.

Collaboration and Teamwork: Evaluating Security Software Tools

With a group of three or four students, use the Web to research and evaluate security products from two competing vendors, such as antivirus software, firewalls, or antispyware software. For each product, describe its capabilities, for what types of businesses it is best suited, and its cost to purchase and install. Which is the best product? Why? If possible, use Google Sites to post links to Web pages, team communication announcements, and work assignments; to brainstorm; and to work collaboratively on project documents. Try to use Google Docs to develop a presentation of your findings for the class.

Are We Ready for Cyberwarfare?

CASE STUDY

For most of us, the Internet is a tool we use for e-mail, news, entertainment, socializing, and shopping. But for computer security experts affiliated with government agencies and private contractors, as well as their hacker counterparts from across the globe, the Internet has become a battlefield—a war zone where cyberwarfare is becoming more frequent and hacking techniques are becoming more advanced. Cyberwarfare poses a unique and daunting set of challenges for security experts, not only in detecting and preventing intrusions but also in tracking down perpetrators and bringing them to justice.

Cyberwarfare can take many forms. Often, hackers use botnets, massive networks of computers that they control thanks to spyware and other malware, to launch large-scale DDoS attacks on their target's servers. Other methods allow intruders to access secure computers remotely and copy or delete e-mail and files from the machine, or even to remotely monitor users of a machine using more sophisticated software. For cybercriminals, the benefit of cyberwarfare is that they can compete with traditional superpowers for a fraction of the cost of, for example, building up a nuclear arsenal. Because more and more modern technological infrastructure will rely on the Internet to function, cyberwarriors will have no shortage of targets at which to take aim.

Cyberwarfare also involves defending against these types of attacks. That's a major focus of U.S. intelligence agencies. While the U.S. is currently at the forefront of cyberwarfare technologies, it's unlikely to maintain technological dominance because of the relatively low cost of the technologies needed to mount these types of attacks.

In fact, hackers worldwide have already begun doing so in earnest. In July 2009, 27 American and South Korean government agencies and other organizations were hit by a DDoS attack. An estimated 65,000 computers belonging to foreign botnets flooded the Web sites with access requests. Affected sites included those of the White House, the Treasury, the Federal Trade Commission, the Defense Department, the Secret Service, the New York Stock Exchange, and the Washington Post, in addition to the Korean Defense Ministry, National Assembly, the presidential Blue House, and several others.

The attacks were not sophisticated, but were widespread and prolonged, succeeding in slowing down most of the U.S. sites and forcing several South Korean sites to stop operating. North Korea or pro-North Korean groups were suspected to be behind the attacks, but the Pyongyang government denied any involvement.

The lone positive from the attacks was that only the Web sites of these agencies were affected. However, other intrusions suggest that hackers already have the potential for much more damaging acts of cyberwarfare. The Federal Aviation Administration (FAA), which oversees the airline activity of the United States, has already been subject to successful attacks on its systems, including one in 2006 that partially shut down air-traffic data systems in Alaska.

In 2007 and 2008, computer spies broke into the Pentagon's $300 billion Joint Strike Fighter project. Intruders were able to copy and siphon off several terabytes of data related to design and electronics systems, potentially making it easier to defend against the fighter when it's eventually produced. The intruders entered through vulnerabilities of two or three contractors working on the fighter jet project. Fortunately, computers containing the most sensitive data were not connected to the Internet, and were therefore inaccessible to the intruders. Former U.S. officials say that this attack originated in China, and that China had been making steady progress in developing online-warfare techniques. China rebutted these claims, stating that the U.S. media was subscribing to outdated, Cold War-era thinking in blaming them, and that Chinese hackers were not skilled enough to perpetrate an attack of that magnitude.

In December 2009, hackers reportedly stole a classified PowerPoint slide file detailing U.S. and South Korean strategy for fighting a war against North Korea. In Iraq, insurgents intercepted Predator drone feeds using software they had downloaded from the Internet.

Earlier that year, in April, cyberspies infiltrated the U.S. electrical grid, using weak points where computers on the grid are connected to the Internet, and left behind software programs whose purpose is unclear, but which presumably could be used to disrupt the system. Reports indicated that the spies

originated in computer networks in China and Russia. Again, both nations denied the charges.

In response to these and other intrusions, the federal government launched a program called "Perfect Citizen" to detect cyberassaults on private companies running critical infrastructure. The U.S. National Security Agency (NSA) plans to install sensors in computer networks for critical infrastructure that would be activated by unusual activity signalling an impending cyberattack. The initial focus will be older large computer control systems that have since been linked to the Internet, making them more vulnerable to cyber attack. NSA will likely start with electric, nuclear, and air-traffic control systems with the greatest impact on national security.

As of this writing, most federal agencies get passing marks for meeting the requirements of the Federal Information Security Management Act, the most recent set of standards passed into law. But as cyberwarfare technologies develop and become more advanced, the standards imposed by this legislation will likely be insufficient to defend against attacks.

In each incident of cyberwarfare, the governments of the countries suspected to be responsible have roundly denied the charges with no repercussions. How could this be possible? The major reason is that tracing identities of specific attackers through cyberspace is next to impossible, making deniability simple.

The real worry for security experts and government officials is an act of cyberwar against a critical resource, such as the electric grid, financial system, or communications systems. First of all, the U.S. has no clear policy about how the country would respond to that level of a cyberattack. Although the electric grid was accessed by hackers, it hasn't yet actually been attacked. A three-year study of U.S. cybersecurity recommended that such a policy be created and made public. It also suggested that the U.S. attempt to find common ground with other nations to join forces in preventing these attacks.

Secondly, the effects of such an attack would likely be devastating. Mike McConnell, the former director of national intelligence, stated that if even a single large American bank were successfully attacked, "it would have an order-of-magnitude greater impact on the global economy" than the World Trade Center attacks, and that "the ability to threaten the U.S. money supply is the equivalent of today's nuclear weapon." Such an attack would have a catastrophic effect on the U.S. financial system, and by extension, the world economy.

Lastly, many industry analysts are concerned that the organization of our cybersecurity is messy, with no clear leader among our intelligence agencies. Several different agencies, including the Pentagon and the NSA, have their sights on being the leading agency in the ongoing efforts to combat cyberwarfare. In June 2009, Secretary of Defense Robert Gates ordered the creation of the first headquarters designed to coordinate government cybersecurity efforts, called Cybercom. Cybercom was activated in May 2010 with the goal of' coordinating the operation and protection of military and Pentagon computer networks in the hopes of resolving this organizational tangle.

In confronting this problem, one critical question has arisen: how much control over enforcing cybersecurity should be given to American spy agencies, since they are prohibited from acting on American soil? Cyberattacks know no borders, so distinguishing between American soil and foreign soil means domestic agencies will be unnecessarily inhibited in their ability to fight cybercrime. For example, if the NSA was investigating the source of a cyberattack on government Web sites, and determined that the attack originated from American servers, under our current laws, it would not be able to investigate further.

Some experts believe that there is no effective way for a domestic agency to conduct computer operations without entering prohibited networks within the United States, or even conducting investigations in countries that are American allies. The NSA has already come under heavy fire for its surveillance actions after 9-11, and this has the potential to raise similar privacy concerns. Preventing terrorist or cyberwar attacks may require examining some e-mail messages from other countries or giving intelligence agencies more access to networks or Internet service providers. There is a need for an open debate about what constitutes a violation of privacy and what is acceptable during 'cyber-wartime', which is essentially all the time. The law may need to be changed to accommodate effective cybersecurity techniques, but it's unclear that this can be done without eroding some privacy rights that we consider essential.

As for these offensive measures, it's unclear as to how strong the United States' offensive capabilities for cyberwarfare are. The government closely guards this information, almost all of which is classified. But former military and intelligence officials indicate that our cyberwarfare capabilities have dramatically increased in sophistication in the past year or two.

And because tracking cybercriminals has proven so difficult, it may be that the best defense is a strong offense.

Sources: "Cyber Task Force Passes Mission to Cyber Command,"Defence Professionals, September 8, 2010; Siobhan Gorman, "U.S. Plans Cyber Shield for Utilities, Companies," *The Wall Street Journal*, July 8, 2010 and "U.S. Hampered in Fighting Cyber Attacks, Report Says," *The Wall Street Journal*, June, 16, 2010; Siobhan Gorman, Yochi Dreazen and August Cole, "Drone Breach Stirs Calls to Fill Cyber Post," *The Wall Street Journal*, December 21, 2009; Sean Gallagher, "New Threats Compel DOD to Rethink Cyber Strategy," *Defense Knowledge Technologies and Net-Enabled Warfare*, January 22, 2010; Lance Whitney, Cyber Command Chief Details Threat to U.S.," *Military Tech*, August 5, 2010; Hoover, J. Nicholas, "Cybersecurity Balancing Act," *Information Week,* April 27, 2009; David E. Sanger, John Markoff, and Thom Shanker, "U.S. Steps Up Effort on Digital Defenses," *The New York Times*, April 28, 2009; John Markoff and Thom Shanker. "Panel Advises Clarifying U.S. Plans on Cyberwar," *The New York Times*, April 30, 2009; Siobhan Gorman and Evan Ramstad, "Cyber Blitz Hits U.S., Korea," *The Wall Street Journal*, July 9, 2009; Lolita C. Baldor, "White House Among Targets of Sweeping Cyber Attack," Associated Press, July 8, 2009; Choe Sang-Hun, "Cyberattacks Hit U.S. and South Korean Web Sites," *The New York Times*, July 9, 2009; Siobhan Gorman, "FAA's Air-Traffic Networks Breached by Hackers," *The Wall Street Journal*, May 7, 2009; Thom Shanker, "New Military Command for Cyberspace," *The New York Times*, June 24, 2009; David E. Sanger and Thom Shanker, "Pentagon Plans New Arm to Wage Wars in Cyberspace," *The New York Times*, May 29, 2009; Siobhan Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *The Wall Street Journal*, April 21, 2009; Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *The Wall Street Journal*, April 8, 2009; "Has Power Grid Been Hacked? U.S. Won't Say," Reuters, April 8, 2009; Markoff, John, "Vast Spy System Loots Computers in 103 Countries." *The New York Times,* March 29, 2009; Markoff, John, "Tracking Cyberspies Through the Web Wilderness," *The New York Times*, May 12, 2009.

CASE STUDY QUESTIONS

1. Is cyberwarfare a serious problem? Why or why not?
2. Assess the management, organization, and technology factors that have created this problem.
3. What solutions have been proposed? Do you think they will be effective? Why or why not?
4. Are there other solutions for this problem that should be pursued? What are they?