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:

Stuxnet and the Changing Face of Cyberwarfare

MWEB Business: Hacked

CHAPTER OUTLINE

YOU'RE ON LINKEDIN? WATCH OUT!

LinkedIn is one of the most prominent social networking sites on the Web. LinkedIn has over 160 million members, mostly career minded white-collar workers more interested in networking than being social. Users maintain online resumes, establish links with their colleagues and business contacts, and search for experts with answers to their daily business problems. People looking for jobs or to advance their careers take this service very seriously. By any measure, LinkedIn has been one of the top tech success stories in the last decade. The company is now valued at over $12 billion.

In June 2012, however, the company suffered a staggering data breach that exposed the passwords of millions of LinkedIn users. Hackers breached LinkedIn's security and stole 6.5 million user passwords, then posted the passwords publicly on a Russian hacking forum. In the aftermath of the breach, LinkedIn users and security experts alike were stunned that a company whose primary function is to collect and manage customer data had done so little to safeguard it. LinkedIn had woefully inadequate computer security, especially for a highly successful tech company with healthy cash reserves, a strong bottom line, and talented employees.

Security experts criticized LinkedIn for not having a chief security officer whose primary job is to guard against security breaches. But even more surprisingly, LinkedIn was found to have minimal password protection via encryption and did not employ several standard encryption techniques used to protect passwords. Most companies will use a technique known as "salting," which adds a series of random digits to the end of hashed passwords to make them more difficult to crack. Salting can be performed at little to no cost with just a few additional lines of code. Most companies use complicated cryptographic functions to salt passwords, but, incredibly LinkedIn had not salted its users' passwords at all, the security equivalent of leaving one's valuables unattended in a crowded area.

Most companies store hashed passwords on separate, secure Web servers to make it more difficult for hackers to break in. The total cost for a company like LinkedIn to set up robust password, Web server, and application security would be in the low six figures, but the average data breach costs companies $5.5 million, according to a Symantec-sponsored study by the Ponemon Institute. LinkedIn's losses might end up being even higher than that, which makes their near total disregard for data security even more surprising.

Some security experts believe that the lack of liability for companies like LinkedIn is a major reason for their lax security policies. Unlike other industries, where basic consumer protections are overseen and protected, computer security and social network data security are not regulated and are poorly protected by many companies. Additionally, with social networks, people tend not to leave a service because of a data breach. For example, in the wake of the breach, many users wanted to leave LinkedIn, but opted not to because it is the most prominent social network for business networking.

© Rafal Olechowski/Shutterstock

Immediately after the password theft, LinkedIn quickly assured its customers that their data were secure. The company disabled the 6.5 million published passwords and announced that it had begun an initiative to salt passwords to increase security. Nevertheless, LinkedIn now faces a $5 million class-action lawsuit that asserts that LinkedIn failed to follow even the minimal industry-standard practices for data protection, specifically more recent forms of salting hashed passwords.

Security experts noted that LinkedIn's security procedures would have been state of the art several years ago, but that they had done little to keep up with and protect themselves from the surge in data breaches in the last year or two. LinkedIn must not only update their security to today's standards, but must also adopt the mindset that protecting consumer data is an ongoing effort, not a one-time fix.

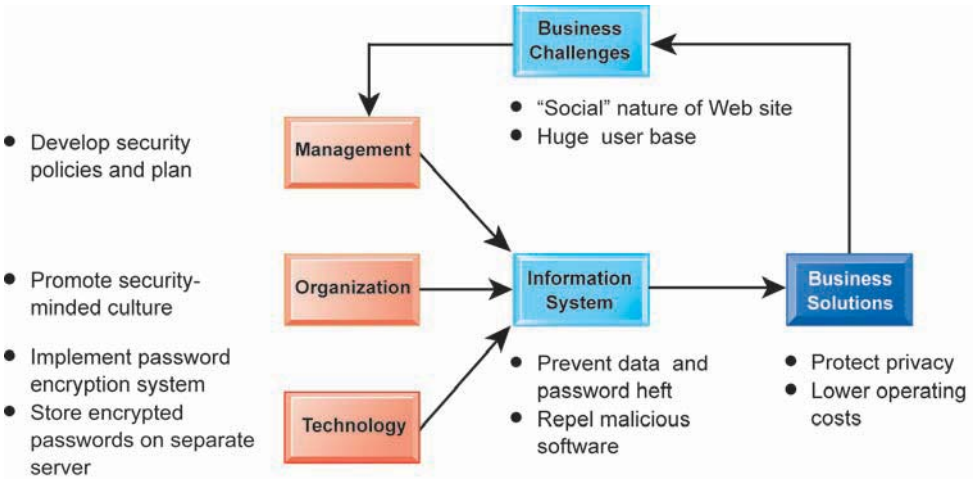
Sources: LinkedIn Faces $5 Million Lawsuit After Password Breach," *CIO Insight*, June 22, 2012; "LinkedIn Defends Reaction in Wake of Password Theft," *The Wall Street Journal*, June 10, 2012; "Lax Security at LinkedIn Is Laid Bare," *The New York Times*, June 10, 2012; "Why ID Thieves Love Social Media," *Marketwatch*, March 25, 2012.

The problems created by the theft of 6.5 million passwords at LinkedIn illustrate some of the reasons why businesses need to pay special attention to information system security. LinkedIn provides important benefits to both individuals and businesses. But from a security standpoint, LinkedIn did not sufficiently protect its Web site from hackers, who were able to steal sensitive user information.

The chapter-opening diagram calls attention to important points raised by this case and this chapter. Although LinkedIn's management has some security technology and procedures in place, it has not done enough to protect its user data. It failed to use standard password encryption techniques, including "salting," to protect user passwords.

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. Given LinkedIn's large user base and the social nature of the site, management did not do enough to protect LinkedIn's data. LinkedIn's loyal user base prevented the fallout from the breach from being much greater, and most people decided they needed to stay with the site because it was so valuable for their careers. Nevertheless, the company faces a multimillion-dollar class action suit as well as reputational damage. For all companies the lesson is clear: difficulties of eradicating malicious software or repairing damage caused by identity theft add to operational costs and make both individuals and businesses less effective.

Here are some questions to think about: What management, organization, and technology factors contributed to the LinkedIn data breach? What was the business impact of the data breach?



8.1 System Vulnerability and Abuse

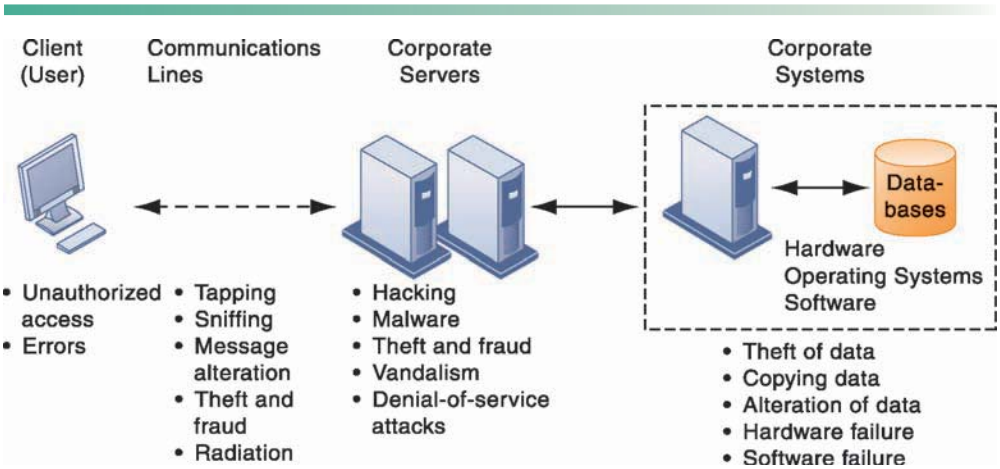
Can you imagine what would happen if you tried to link to the Internet without a firewall or antivirus software? Your computer would be disabled in a few seconds, and it might take you many days to recover. If you used the computer to run your business, you might not be able to sell to your customers 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

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.

layer can cause harm by introducing errors or by accessing systems without 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. Smartphones used by corporate employees often contain sensitive data such as sales figures, customer names, phone numbers, and e-mail addresses. Intruders may be able to access internal corporate systems 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 information 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.

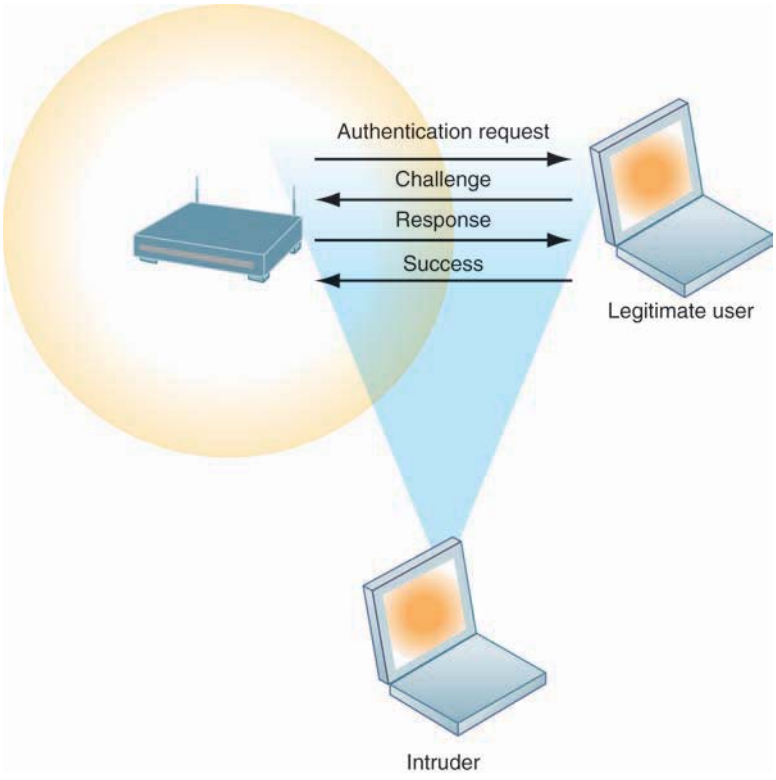
Wireless Security Challenges

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. 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)* that identify 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**, in which eavesdroppers drive by buildings or park outside and try to intercept wireless network traffic.

An intruder that has associated with an access point by using the correct SSID is capable of accessing other resources on the network. For example, the intruder could use 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.

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.

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 network interface controller (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.

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 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, worms 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, online ads, or instant messaging. Viruses have also invaded computerized information systems from "infected" disks or infected machines. Especially prevalent today are **drive-by downloads**, consisting of malware that comes with a downloaded file that a user intentionally or unintentionally requests.

Hackers can do to a smartphone just about anything they can do to any Internet device: request malicious files without user intervention, delete files, transmit files, install programs running in the background to monitor user actions, and potentially convert the smartphone into a robot in a botnet to send e-mail and text messages to anyone. With smartphones starting to outsell PCs, and smartphones increasingly used as payment devices, they are becoming a major avenue for malware.

Malware targeting mobile devices is not yet as extensive as that targeting larger computers, but nonetheless is spreading using e-mail, text messages, Bluetooth, and file downloads from the Web via Wi-Fi or cellular networks. The security firm McAfee found nearly 13,000 different kinds of malware targeting mobile devices in 2012 compared to less than 2,000 in 2011, with almost all attacks targeting devices using Google's Android operating system. (Graziano, 2012). Mobile device viruses pose serious threats to enterprise computing because so many wireless devices are now linked to corporate information systems.

Blogs, wikis, and social networking sites such as Facebook 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. On July 4, 2011, hackers broke into the "Fox News Politics" Twitter account, sending fake messages about President Barack Obama. The hackers changed the account's password, preventing Fox from correcting the messages for hours (Sherr, 2011).

Internet security firm Symantec reported in 2012 that it had detected 403 million new and unique threats from malicious software in 2011, up from 286 million in 2010. Symantec observed that the amount of harmful software in the world passed the amount of beneficial software in 2007, and as many as one of every 10 downloads from the Web includes harmful programs (Drew and Kopytoff, 2011). According to Symantec, 36 percent of malware today is being targeted at small businesses, because it is more difficult for such companies to protect themselves against so many different types of attacks (Symantec, 2012). Table 8.1 describes the characteristics of some of the most harmful worms and viruses that have appeared to date.

A **Trojan horse** is a software program that appears to be benign but then does something other than expected. 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

TABLE 8.1 EXAMPLES OF MALICIOUS CODE

NAME	TYPE	DESCRIPTION
Conficker (aka Downadup, Downup)	Worm	First detected in November 2008 and still prevalent. Uses flaws in Windows software to take over machines and link them into a virtual computer that can be commanded remotely. Had 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.

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.

An example of a modern-day Trojan horse is the MMarketPay.A Trojan for Android phones. This Trojan is hidden in several apps that appear to be legitimate, including travel and weather apps. It places orders for applications and movies automatically without the user's permission, potentially causing users to be hit with unexpectedly high phone bills. MMarketPay.A has been detected in multiple app stores and has spread to more than 100,000 devices.

SQL injection attacks have become a major 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. For example, the Zeus Trojan stole financial and personal data from online banking and social networking sites by surreptitiously tracking users' keystrokes as they entered data into their computers. Other spyware programs reset Web browser home pages, redirect search requests, or slow performance by taking up too much memory.

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 and 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, hours after the U.S. Department of Justice shut down file-sharing site Megaupload on January 19 2012, the Anonymous hacker collective launched extensive retaliatory DDoS attacks against federal and entertainment industry Web sites. Web sites belonging to the FBI, U.S. Department of Justice, U.S. Copyright Office, Universal Music, the Recording Industry Association of America, and the Motion Picture Association of America, were knocked offline for a large part of the day.

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 DDoS 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 hackers infect enough computers, they can use the amassed resources of the botnet to launch DDos attacks, phishing campaigns, or unsolicited "spam" e-mail.

Ninety percent of the world's spam and 80 percent of the world's malware are delivered via botnets. For example, the Grum botnet, once the world's third-largest botnet, was reportedly responsible for 18% of worldwide spam traffic (amounting to 18 billion spam messages per day) when it was shut down on July 19, 2012. At one point Grum had infected and controlled 560,000–840,000 computers.

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. In November, 2010, New York resident George Castro was charged with grand larceny for allegedly stealing nearly $4.5 million from Columbia University over the course of two months. Castro had added a TD Bank account belonging to him as a payee in the Columbia University Medical Center's accounts payable system (El-Ghobashy, 2010). 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 both a target and 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 Ponemon Institute's Second Annual Cost of Cyber Crime Study sponsored by ArcSight, the median annualized cost of cybercrime for the organizations in the study was $5.9 million per year (Ponemon Institute, 2011). 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 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.

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

Identify theft has flourished on the Internet, with credit card files a major target of Web site hackers. According to the Identity Fraud Report by Javelin Strategy & Research, identity theft increased by 13 percent in 2011, with the total number of victims increasing to 11.6 million adults. However, the total dollar losses from identity theft have remained steady at about $18 billion (Javelin, 2012). 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 messages that look like those of legitimate businesses to ask users for confidential personal data. The e-mail 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. In a more targeted form of phishing called *spear phishing,* messages appear to come from a trusted source, such as an individual within the recipient's own company or a friend.

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.

According to the Ponemon Institute's seventh annual U.S. Cost of a Data Breach Study, data breach incidents cost U.S. companies $194 per compromised customer record in 2011. The average total per-incident cost in 2011 was $5.5 million (Strom, 2012). Additionally, brand damage can be significant, albeit hard to quantify. Table 8.3 describes the most expensive data breaches that have occurred to date.

The U.S. Congress addressed the threat of computer crime in 1986 with the Computer Fraud and Abuse Act, which makes it illegal to access a computer system without authorization. Most states have similar laws, and nations in Europe have comparable legislation. Congress passed the National Information Infrastructure Protection Act in 1996 to make malware distribution and hacker attacks to 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. A proposed federal Data Security and Breach Notification Act would mandate organizations that possess personal information to put in place

TABLE 8.3 THE FIVE MOST EXPENSIVE DATA BREACHES

DATA BREACH	DESCRIPTION
U.S. Veterans Affairs Department	In 2006, the names, birth dates, and social security numbers of 17.5 million military veterans and personnel were stolen from a laptop that a Department of Veterans Affairs employee had taken home. The VA spent at least $25 million to run call centers, send out mailings, and pay for a year of a credit-monitoring service for victims.
Heartland Payment Systems	In 2008, criminals led by Miami hacker Albert Gonzales installed spying software on the computer network of Heartland Payment Systems, a payment processor based in Princeton, NJ, and stole the numbers of as many as 100 million credit and debit cards. Gonzales was sentenced in 2010 to 20 years in federal prison, and Heartland paid about $140 million in fines and settlements.
TJX	A 2007 data breach at TJX, the retailer that owns national chains including TJ Maxx and Marshalls, cost at least $250 million. Cyber criminals took more than 45 million credit and debit card numbers, some of which were used later to buy millions of dollars in electronics from Walmart and elsewhere. Albert Gonzales, who played a major role in the Heartland hack, was linked to this cyberattack as well.
Epsilon	In March 2011, hackers stole millions of names and e-mail addresses from the Epsilon e-mail marketing firm, which handles e-mail lists for major retailers and banks like Best Buy, JPMorgan, TiVo, and Walgreens. Costs could range from $100 million to $4 billion, depending on what happens to the stolen data, with most of the costs from losing customers due to a damaged reputation.
Sony	In April 2011, hackers obtained personal information, including credit, debit, and bank account numbers, from over 100 million PlayStation Network users and Sony Online Entertainment users. The breach could cost Sony and credit card issuers up to a total of $2 billion.

"reasonable" security procedures to keep the data secure and to notify anyone affected by a data breach, but it has not been enacted.

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 cyber criminal activities we have described—launching malware, denial-of-service attacks, and phishing probes—are borderless. China, the United States, South Korea, Russia, and Taiwan are currently the sources of most of the world's malware (King, 2012). The global nature of the Internet makes it possible for cybercriminals to operate—and to do harm—anywhere in the world.

Internet vulnerabilities have also turned individuals and even entire nation states into easy targets for politically-motivated hacking to conduct sabotage and espionage. **Cyberwarfare** is a state-sponsored activity designed to cripple and defeat another state or nation by penetrating its computers or networks for the purposes of causing damage and disruption.

In general, cyberwarfare attacks have become much more widespread, sophisticated, and potentially devastating. There are 250,000 probes trying to find their way into the U.S. Department of Defense networks every hour, and cyberattacks on U.S. federal agencies have increased 150 percent since 2008. Over the years, hackers have stolen plans for missile tracking systems, satellite navigation devices, surveillance drones, and leading-edge jet fighters.

Cyberwarfare poses a serious threat to the infrastructure of modern societies, since their major financial, health, government, and industrial institutions rely on the Internet for daily operations. Cyberwarfare also involves defending against these types of attacks. The Interactive Session on Organizations describes some recent cyberwarfare attacks and their growing sophistication and severity.

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 software error in an iPad app for paying bills caused Citibank to double the charge for customer payments between July and December 2011. Some customers using their iPads to settle their cable bill or mortgage payment, for example, actually paid twice (Protess, 2012).

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

INTERACTIVE SESSION: ORGANIZATIONS

STUXNET AND THE CHANGING FACE OF CYBERWARFARE

In July 2010, reports surfaced about a Stuxnet worm that had been targeting Iran's nuclear facilities. In November of that year, Iran's President Mahmoud Ahmadinejad publicly acknowledged that malicious software had infected the Iranian nuclear facilities and disrupted the nuclear program by disabling the facilities' centrifuges. Stuxnet had earned its place in history as the first visible example of industrial cyberwarfare.

To date, Stuxnet is the most sophisticated cyberweapon ever deployed. Stuxnet's mission was to activate only computers that ran Supervisory Control and Data Acquisition (SCADA) software used in Siemens centrifuges to enrich uranium. The Windows-based worm had a "dual warhead." One part was designed to lay dormant for long periods, then speed up Iran's nuclear centrifuges so that they spun wildly out of control. Another secretly recorded what normal operations at the nuclear plant looked like and then played those recordings back to plant operators so it would appear that the centrifuges were operating normally when they were actually tearing themselves apart.

The worm's sophistication indicated the work of highly skilled professionals. Michael Assante, president and CEO at the National Board of Information Security Examiners, views Stuxnet as a weapons delivery system like the B-2 Bomber. The software program code was highly modular, so that it could be easily changed to attack different systems. Stuxnet only became active when it encountered a specific configuration of controllers, running a set of processes limited to centrifuge plants.

Over 60 percent of Stuxet-infected computers are in Iran, and digital security company Kaspersky Labs speculates that the worm was launched with nation-state support (probably from Israel and the United States) with the intention of disabling some or all of Iran's uranium enrichment program. Stuxnet wiped out about one-fifth of Iran's nuclear centrifuges. The damage was irreparable and is believed to have delayed Iran's ability to make nuclear arms by as much as five years. And no one is certain that the Stuxnet attacks are over. Some experts who examined the Stuxnet software code believe it contains the seeds for more versions and attacks.

According to a Tofino Security report, Stuxnet is capable of infecting even well-secured computer systems that follow industry best practices. Companies' need for interonnectivity between control systems make it nearly impossible to defend against a well-constructed, multi-pronged attack such as Stuxnet.

And Stuxnet is not the only cyberweapon currently at work. The Flame virus, released about five years ago, has been infecting computers in Iran, Lebanon, Sudan, Saudi Arabia, Egypt, Syria, and Israel. While researchers are still analyzing the program, the attack's main goal is stealing information and espionage. Flame is able to grab images of users' computer screens, record their instant messaging chats, collect passwords, remotely turn on their microphones to record audio conversations, scan disks for specific files, and monitor their keystrokes and network traffic. The software also records Skype conversations and can turn infected computers into Bluetooth beacons which attempt to download contact information from nearby Bluetooth-enabled devices These data, along with locally stored documents, can be sent to one of several command and control servers that are scattered around the world. The program then awaits further instructions from these servers.

The Duqu worm, discovered in September 2011, also aims to steal information by scanning systems. Duqu infects a very small number of very specific systems around the world, but may use completely different modules for infiltrating those separate systems. One of Duqu's actions is to steal digital certificates used for authentication from attacked computers to help future viruses appear as secure software. It is going largely undetected. Security researchers believe Duqu was created by the same group of programmers behind Stuxnet.

The real worry for security experts and government officials is an act of cyberwarfare against a critical resource, such as the electric grid, financial systems, or communications systems. (In April 2009, 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.)

The U.S. has no clear strategy about how the country would respond to that level of cyberattack, and the effects of such an attack would likely be devastating. Mike McConnell, the former director of national intel-

ligence, 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 financial equivalent of a nuclear weapon.

Many security experts believe that U.S. cybersecurity is not well-organized. Several different agencies, including the Pentagon and the National Security Agency (NSA), have their sights on being the leading agency in the ongoing efforts to combat cyberwarfare. The first headquarters designed to coordinate government cybersecurity efforts, called Cybercom, was activated in May 2010 in the hope of resolving this organizational tangle. In May 2011 President Barack Obama signed executive orders weaving cyber capabilities into U.S. military strategy, but these capabilities are still evolving. Will the United States and other nations be ready when the next Stuxnet appears?

Sources: Brian Royer, "Stuxnet, The Nation's Power Grid, And The Law Of Unintended Consequences, *Dark Reading*, March 12, 2012; Thomas Erdbrink, "Iran Confirms Attack by Virus That Collects Information," *The New York Times*, May 29, 2012; Nicole Perlroth, "Virus Infects Computers Across Middle East," *The New York Times*, May 28, 2012; Thom Shanker and Elisabeth Bumiller, "After Suffering Damaging Cyberattack, the Pentagon Takes Defensive Action," *The New York Times,* July 15, 2011; Robert Leos, "Secure Best Practices No Proof Against Stuxnet," CSO, March 3, 2011; Lolita C. Baldor, "Pentagon Gets Cyberwar Guidelines," Associated Press, June 22, 2011; William J. Broad, John Markoff, and David E. Sanger, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay," *The New York Times*, January 15, 2011; George V. Hulme, "SCADA Insecurity" and Michael S. Mimoso, "Cyberspace Has Gone Offensive," *Information Security's Essential Guide to Threat Management* (June 14, 2011); and Sibhan Gorman and Julian A. Barnes, "Cyber Combat: Act of War," *The Wall Street Journal*, May 31, 2011.

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 makes Stuxnet different from other cyberwarfare attacks? How serious a threat is this technology?
4. What solutions for have been proposed for this problem? Do you think they will be effective? Why or why not?

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 2011, Symantec identified 351 browser vulnerabilities: 70 in Chrome, about 50 in Safari and Firefox, and 50 in Internet Explorer. Some of these vulnerabilities were critical (Symantec, 2012).

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 7 Service Pack 1, which features security, performance, and stability updates for Windows 7. 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.

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. Systems that are unable to function because of security breaches, disasters, or malfunctioning technology can permanently impact a company's financial health. Some experts believe that 40 percent of all businesses will not recover from application or data losses that are not repaired within three days (Focus Research, 2010).

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 storage devices, 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 general 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 8.4 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 the results of computer processing are accurate, complete, and properly distributed.

TABLE 8.4 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.

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 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 8.5 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,

TABLE 8.5 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

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.

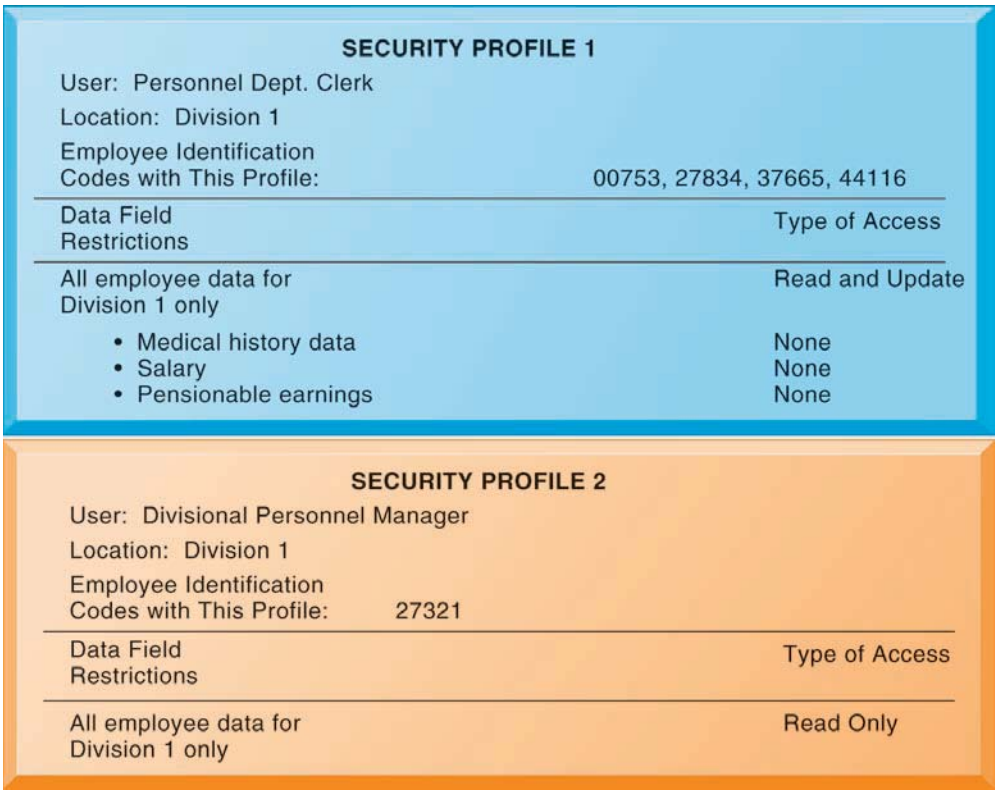
SECURITY POLICY

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 other 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 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 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 security profile, a user would have certain restrictions on access to various systems, locations, or data in an organization.

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 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

FIGURE 8.4 SAMPLE AUDITOR'S LIST OF CONTROL WEAKNESSES

Function: Loans **Location: Peoria, IL**	**Prepared by: J. Ericson** **Date: June 16, 2013**		**Received by: T. Benson** **Review date: June 28, 2013**	
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	5/10/13	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	5/10/13	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.

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.

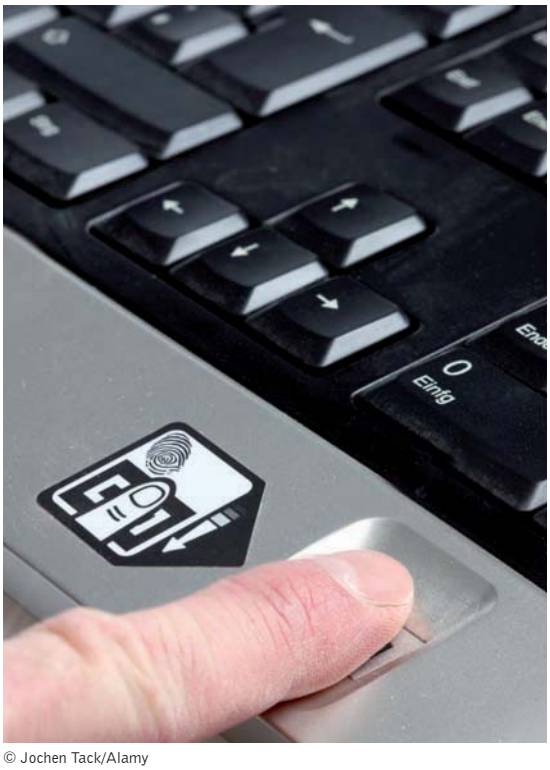
IDENTITY MANAGEMENT AND AUTHENTICATION

Midsize and large 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 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 keeping 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 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.



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.

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.

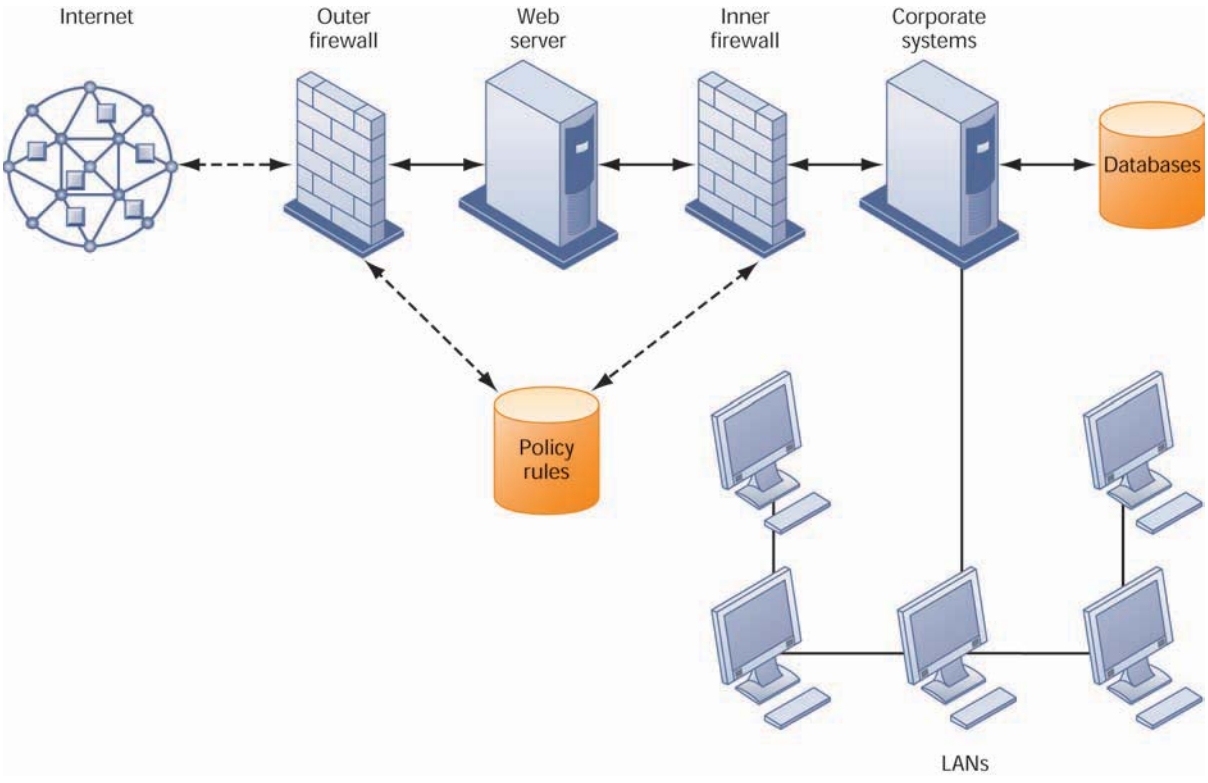
Firewalls

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

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.

Address Translation, and application proxy filtering. They are frequently used in combination to provide firewall protection.

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 anti-malware protection for every computer. **Antivirus software** prevents, detects, and removes malware, including computer viruses, computer worms, Trojan horses, spyware, and adware. However, most antivirus software is effective only against malware already known when the software was written. To remain effective, the antivirus software must be continually updated.

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 businesses, 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

The initial security standard developed for Wi-Fi, called Wired Equivalent Privacy (WEP), is not very effective because its encryption keys are relatively easy to crack. WEP provides some margin of security, however, if users remember to enable 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 authentication 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, communicators 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.

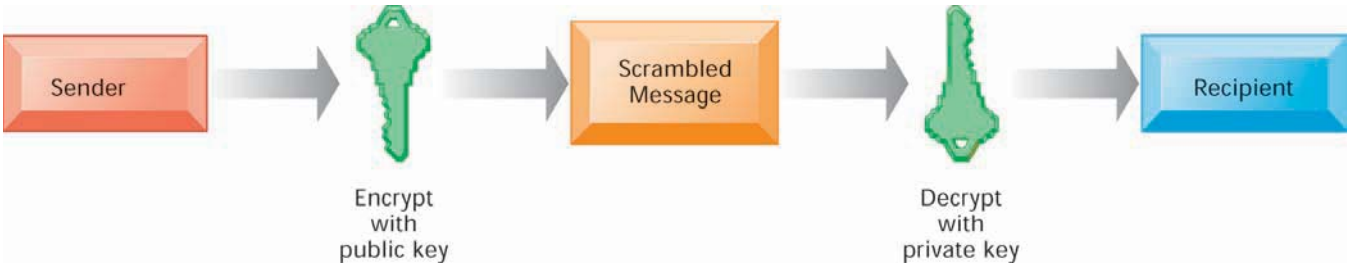
Digital certificates are data files used to establish the identity of users and electronic assets for protection of online transactions (see Figure 8.7). A digital certificate system uses a trusted third party, known as a certificate authority (CA, or certification authority), to validate a user's identity. There are many CAs in the United States and around the world, including Symantec, GoDaddy, and Comodo.

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 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

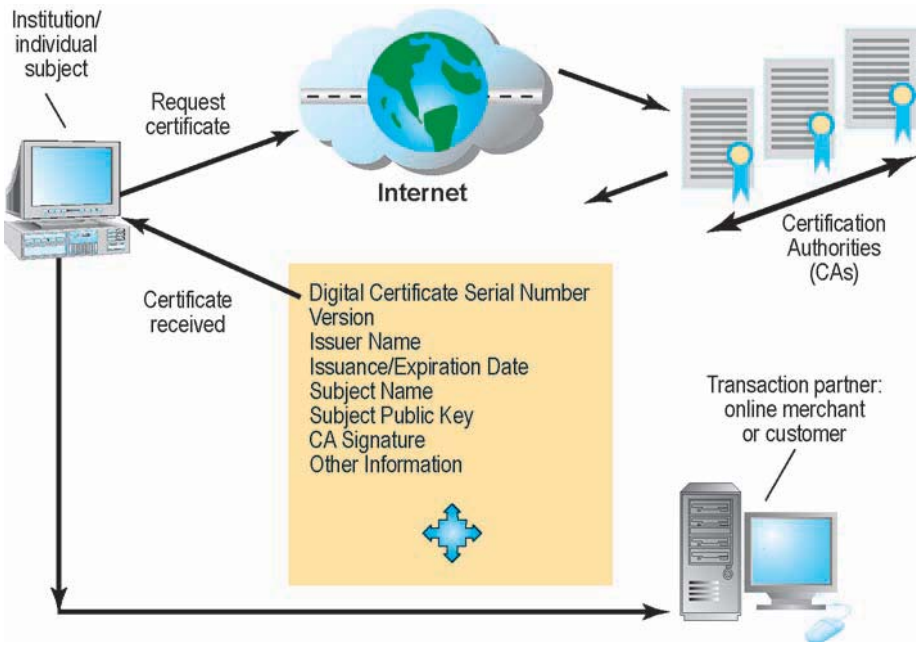
As companies increasingly rely on digital networks for revenue and operations, they need to take additional steps to ensure that their systems and applications are always available. Firms such as those in the airline and financial services industries with critical applications requiring online transaction processing have traditionally used fault-tolerant computer systems for many years to ensure 100

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.

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.

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 State University in Muncie, Indiana, found its network had slowed because a small minority of students were using P2P 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 describes how even sophisticated Web-based firms can experience security breakdowns.

Cloud computing is highly distributed. Cloud applications reside 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.

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.

Companies expect their systems to be running 24/7, but cloud providers haven't always been able to provide this level of service. On several occasions

over the past few years, the cloud services of Amazon.com and Salesforce.com experienced outages that disrupted business operations for millions of users (see the Chapter 5 ending case study).

Cloud users need to confirm that regardless of where their data are stored, 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 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 mobile device management 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 or erase lost or stolen 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 should encrypt communication whenever possible. All mobile device users should be required to use the password feature found in every smartphone. Mobile security products are available from Kaspersky, Lookout, and DroidSecurity.

Some companies insist that employees use only company-issued smartphones. BlackBerry devices are considered the most secure because they run within their own secure system. But, increasingly, companies are allowing employees to use their own smartphones, including iPhones and Android phones, for work, to make employees more available and productive (see the Chapter 5 discussion of BYOD). Protective software products, such as the tools from Good Technology, are now available for segregating corporate data housed within personally owned mobile devices from the device's personal content.

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 the information systems department and end users to jointly measure the performance of the system and identify problems as they occur. Examples

INTERACTIVE SESSION: TECHNOLOGY

MWEB BUSINESS: HACKED

MWEB, launched in 1997, became South Africa's leading ISP in 1998. It has established itself as a company that provides a cutting-edge network and service infrastructure and outstanding customer service. Currently, MWEB's customer base of 320,000 includes home users; small, medium, and large business customers; and corporate clients. MWEB won the ISP of the Year award at the MyBroadband Conference in Johannesburg in 2010. The award was based on the performance of its various broadband services as well as on customer satisfaction.

Its business division, MWEB Business, was founded in January 1998. MWEB Business prides itself as being a business partner that is perfectly positioned to leverage the power of Web-based technologies in all areas of an organization. MWEB Business helps companies:

- Manage business data in ways that add real value and insight to their operations
- Integrate existing systems with the Internet so as to close the gap between technology, strategy, and the organization's bottom line
- Develop, manage, and maintain solutions that include all aspects of Internet connectivity, Web site development and hosting, broadband and wireless applications, e-commerce, and consultancy services
- Manage internal information among employees, as well as among business partners and suppliers

MWEB has moved forward in publicizing its plans for the South African Internet market. According to MWEB CEO Rudi Jansen, the company needs to improve the quality of their network, which is not only an MWEB problem, but also a Telkom network problem. Despite having a less-than-ideal network infrastructure, MWEB uses AVG Internet Security to offer its customers the best possible security while online. AVG Internet Security offers MWEB customers the following features:

- Identity protection for safe banking and shopping
- LinkScanner for safe surfing and searching
- WebShield for safe social networking, chatting, and downloading
- Antiphishing and antispam for a safe uncluttered inbox
- High-speed antivirus/antispyware software with automatic updates
- An enhanced firewall

In addition, MWEB automatically protects customers against junk email and viruses that are sent via email. Its virus filter ensures that only virus-free email is delivered to clients' inboxes by automatically cleaning e-mails from recognized malware sources. MWEB advises its customers to keep their ADSL connections safe from bandwidth theft and account abuse by blocking unsolicited incoming connections to network ports commonly used by hackers.

Despite the multitude of security services offered by MWEB, a number of MWEB Business subscribers' account details were compromised when their logon and password details were published on the Internet by hackers. Initial reports indicated that as many as 2,390 users of MWEB's business digital subscriber lines were affected. The company disclosed the security breach on October 25, 2010. It appears that hackers gained access to the Internet Solutions' self-service management system that MWEB Business uses to provide and manage business accounts that have not yet been migrated to the MWEB network.

Historically, MWEB Business was a reseller of Internet Solutions' Uncapped & Fixed IP ADSL services, which were provisioned and managed by MWEB using a Web-based management interface provided by Internet Solutions. All new Business ADSL services provided after April 2010, as well as the bulk of legacy services already migrated, used MWEB's internal authentication systems, which were completely unaffected by this incident.

MWEB responded quickly to the hacking incident. According to Jansen, about 1,000 clients on the Internet Solutions network needed to be migrated from the old server which was attacked by hackers. Although the network was quickly secured, most customers had recently been moved to MWEB's IPC network. MWEB would also be contacting these customers to reset their passwords, as an added security measure. Jansen was quick to note that no personal information was lost and that none of MWEB's clients suffered any losses as their usernames and passwords had been recreated and changed. He further added that MWEB successfully repels 5,000 attacks a day.

Andre Joubert, general manager of MWEB Business, emphasized that only ADSL authentication usernames and passwords had been compromised. The integrity of the personal or private data related to the accounts remained intact, as did the access credentials for each customer's bundled onsite router. Joubert did acknowledge the seriousness of the hack, apologizing for any inconvenience the breach may have caused to MWEB's customers. As soon as the breach was identified, MWEB took immediate action to evaluate the extent of the breach and to limit any damage. In MWEB's defense, Jansen said that MWEB constantly advises its customers to be vigilant regarding their online data and security. In addition, MWEB was working closely with Internet Solutions to investigate the nature and source of the breach to ensure that it does not happen again.

Sources: "2010 MyBroadband Awards: The Winners and Losers," MyBroadband, October 19, 2010 (http://mybroadband.co.za/news/ broadband/15951-2010-MyBroadband-Awards-The-winners-andlosers. html, accessed November 17, 2010); "About MWEB," MWEB (www.mweb.co.za/productspricing/MWEBBusiness/AboutMWEBB usiness.aspx, accessed November 17, 2010); "Hackers Target MWEB," NewsTime, October 25, 2010 (www.newstime.co.za/ ScienceandTech/Hackers_Target_M-Web/13618/, accessed November 17, 2010); "MWEB Business Tackles 'ADSL Hacking' Incident," MyBroadband, October 25, 2010 (http://mybroadband.co.za/news/adsl/16077-MWEB-Businesstackles- ADSL-hacking-incident.html, accessed November 17, 2010); "MWEB Business Takes Action in 'Hacking' Incident," Moneyweb, October 25, 2010 (www.moneyweb.co.za/mw/view/mw/en/ page295027?oid=5 12545&sn=2009+Detail&pid=287226, accessed November 17, 2010); "MWeb hacked, users' details exposed," TechCentral, October 26, 2010 (www.techcentral.co.za/mwebhacked- users-details-exposed/18366/, accessed November 17, 2010).

Case contributed by Upasana Singh, University of KwaZulu-Natal

CASE STUDY QUESTIONS

1. What technology issues led to the security breach at MWEB?
2. What is the possible business impact of this security breach for both MWEB and its customers?
3. If you were an MWEB customer, would you consider MWEB's response to the security breach to be acceptable? Why or why not?
4. What should MWEB do in the future to avoid similar incidents?

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 11. Our Learning Tracks also contain descriptions of methodologies for developing software programs that also contribute to software quality.

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), 342
Antivirus software, 348
Application controls, 340
Authentication, 346
Biometric authentication, 346
Botnet, 331
Bugs, 335
Business continuity planning, 344
Click fraud, 334
Computer crime, 332
Computer forensics, 339
Computer virus, 328
Controls, 325
Cybervandalism, 330
Cyberwarfare, 334
Deep packet inspection (DPI), 352
Denial-of-service (DoS) attack, 331
Digital certificates, 350
Disaster recovery planning, 344
Distributed denial-of-service (DDoS) attack, 331
Downtime, 351
Drive-by download, 328
Encryption, 349
Evil twin, 333
Fault-tolerant computer systems, 351
Firewall, 347
General controls, 340
Gramm-Leach-Bliley Act, 339
Hacker, 330
High-availability computing, 351
HIPAA, 338
Identity management, 342
Identity theft, 332
Intrusion detection systems, 348
Keyloggers, 330
Malware, 328
Managed security service providers (MSSPs), 352
MIS audit, 344
Online transaction processing, 351
Password, 346
Patches, 337
Pharming, 333
Phishing, 333
Public key encryption, 350
Public key infrastructure (PKI), 350
Recovery-oriented computing, 351
Risk assessment, 341
Sarbanes-Oxley Act, 339
Secure Hypertext Transfer Protocol (S-HTTP), 349
Secure Sockets Layer (SSL), 349
Security, 325
Security policy, 342
Smart card, 346
Sniffer, 331
Social engineering, 335
Spoofing, 331
Spyware, 330
SQL injection attack, 330
Token, 346
Trojan horse, 329
Unified threat management (UTM), 349
War driving, 327
Worms, 328

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 tolerance 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?

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 IT infastructure has identified a number of security vulnerabilities. Review the data on these vulnerabilities, which can be found in a table in MyMISLab. Use the table to answer the following questions:

   - 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 paint manufacturing company located in Alabama that uses a network to link its business operations. A security risk assessment requested by management identified a number of potential exposures. These exposures, their associated probabilities, and average losses are summarized in a table, which can be found in MyMISLab. Use the table to answer the following questions:

- In addition to the potential exposures listed, 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

This project will help develop your Internet skills in using the Web to research and evaluate security outsourcing services.

You have been asked to help your company's 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 you selected and justify your decision.

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 Project

In MyMISLab you will find a Collaboration and Teamwork Project dealing with the concepts in this chapter. You will be able to use Google Sites, Google Docs, and other open source collaboration tools to complete the assignment.

Information Security Threats and Policies in Europe
CASE STUDY

The IT sector is one of the key drivers of the European economy. It has been estimated that 60 percent of Europeans use the Internet regularly. Additionally, 87 percent own or have access to mobile phones. In 2009, the European broadband market was the largest in the world. These facts demonstrate the importance of ensuring the security and safe operation of the Internet for the well-being of the European economy. The safety and security of the Internet have been threatened in recent years, as Internet-based cyber attacks have become increasingly sophisticated.

In 2007, Estonia suffered a massive cyber attack that affected the government, the banking system, media, and other services. The attack was performed using a variety of techniques, ranging from simple individual ping commands and message flooding to more sophisticated distributed denial of service (DDoS) attacks. Hackers coordinated the attack by using a large number of compromised servers organized in a botnet distributed around the world. A botnet is a network of autonomous malicious software agents that are under the control of a bot commander. The network is created by installing malware that exploits the vulnerabilities of Web servers, operating systems, or applications to take control of the infected computers. Once a computer is infected it becomes part of a network of thousands of "zombies," machines that are commanded to carry out the attack.

The cyber attack on Estonia started in late April 2007 and lasted for almost 3 weeks. During this period, vital parts of the Estonian Internet network had to be closed from access from outside the country, causing millions of dollars in economic losses.

At around the same time, Arsys, an important Spanish domain registration company, was also targeted by international hackers. Arsys reported that hackers had stolen codes that were then used to insert links to external servers containing malicious codes in the Web pages of some of its clients.

In 2009, an estimated 10 million computers were infected with the Conflicker worm worldwide. France, the UK, and Germany were among the European countries that suffered the most infections. The French navy had to ground all military planes when it was discovered that its computer network was infected. In the UK, the worm infected computers in the Ministry of Defense, the city of Manchester's city council and police IT network, some hospitals in the city of Sheffield, and other government offices across the country. Computers in the network of the German army were also reported as infected. Once installed on a computer, Conflicker is able to download and install other malware from controlled Web sites, thus infected computers could be under full control of the hackers.

More recently, a sophisticated malware threat targeting industrial systems was detected in Germany, Norway, China, Iran, India, Indonesia, and other countries. The malware, known as Stuxnet, infected Windows PCs running the Supervisory Control and Data Acquisition (SCADA) control system from the German company Siemens. Stuxnet was propagated via USB devices. Experts estimated that up to 1,000 machines were infected on a daily basis at the peak of the infection. The malware, hidden in shortcuts to executable programs (files with extension .lnk), was executed automatically when the content of an infected USB drive was displayed. Employing this same technique, the worm was capable of installing other malware. Initially, security experts disclosed that Stuxnet was designed to steal industrial secrets from SIMATIC WinCC, a visualization and control software system from Siemens. However, data gathered later by other experts indicates that the worm was actually looking for some specific Programmable Logic Controllers (PLC) devices used in a specific industrial plant, a fact that points to the possibility that the malware was part of a well-planned act of sabotage. Even though none of the sites infected with Stuxnet suffered physical damage, the significance that such a sophisticated threat represents to the industrial resources in Europe and other parts of the world cannot be underestimated.

As of 2001, EU member states had independent groups of experts that were responsible for responding to incidents in information security. These groups lacked coordination and did not exchange much information. To overcome this, in 2004 the European Commission established the European Network and Information Security Agency (ENISA) with the goal of coordinating efforts to prevent and respond more effectively to potentially more harmful security threats. ENISA's main objectives are to secure

Europe's information infrastructure, promote security standards, and educate the general public about security issues.

ENISA organized the first pan-European Critical Information Infrastructure Protection (CIIP) exercise, which took place in November 2010. This exercise tested the efficiency of procedures and communication links between member states in case an incident were to occur that would affect the normal operation of the Internet. ENISA acts as a facilitator and information broker for the Computer Emergency Response Teams (CERT), working with the public and private sectors of most EU member states.

The European Commission has recently launched the Digital Agenda for Europe. The goal of this initiative is to define the key role that information and communication technologies will play in 2020. The initiative calls for a single, open European digital market. Another goal is that broadband speeds of 30Mbps be available to all European citizens by 2020. In terms of security, the initiative is considering the implementation of measures to protect privacy and the establishment of a well-functioning network of CERT to prevent cybercrime and respond effectively to cyber attacks.

Sources: "Digital Agenda for Europe," European Commission, August 2010 (http://ec.europa.eu/information_society/ digitalagenda/ index_en.htm, accessed October 20, 2010); "The Cyber Raiders Hitting Estonia," BBC News, May 17, 2007 (http://news.bbc.co.uk/2/hi/europe/6665195.stm, accessed November 17, 2010); Robert McMillan, "Estonia Ready for the Next Cyberattack," Computerworld, April 7, 2010 (www.computerworld. com/s/article/9174923/Estonia_readies_for_the_next_cyber attack, accessed November 17, 2010); "Another Cyber Attack Hits Europe," Internet Business Law Services, June 18, 2007 (www.ibls.com/internet_law_news_portal_view.aspx?id=1782&s= latestnews, accessed November 17, 2010); "New Cyber Attack Hits Norway," Views and News from Norway, August 30, 2010 (www.newsinenglish.no/2010/08/30/new-cyber-attacks-hit-norway, accessed November 17, 2010); Gregg Keiser, "Is Stuxnet the 'Best' Malware Ever?" Computerworld, September 16, 2010; Robert McMillan, "Was Stuxnet Built to Attack Iran's Nuclear Program," Computerworld, September 21 2010 (www.computerworld.com/s/article/9186920/Was_Stuxnet_built_to_attack_Iran_s_nuclear_program_, accessed November 17, 2010); Ellen Messmer, "Downadup/Conflicker Worm. When Will the Next Shoe Fall?" Network World, January 23 2009 (www.networkworld.com/news/2009/012309-downadup-conflicker-worm.html?hpg1=bn, accessed November 17, 2010); Erik Larkin, "Protecting Against the Rampant Conflicker Worm," PCWorld, January 16, 2009; "War in the Fifth Domain," The Economist, July 1, 2010 (www.economist.com/node/16478792, accessed November 17, 2010).

CASE STUDY QUESTIONS

1. What is a botnet?
2. Describe some of the main points of the Digital Agenda for Europe.
3. Explain how a cyber attack can be carried out.
4. Describe some of the weaknesses exploited by malware.

Case contributed by Daniel Ortiz-Arroyo, Aalborg University