CHAPTER

8 Securing Information Systems

LEARNING OBJECTIVES

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

8-1 Why are information systems vulnerable to destruction, error, and abuse?

8-2 What is the business value of security and control?

8-3 What are the components of an organizational framework for security and control?

8-4 What are the most important tools and technologies for safeguarding information resources?

8-5 How will MIS help my career?

CHAPTER CASES

Cyberattacks in the Asia-Pacific Target the Weakest Link: People

Capital One: A Big Bank Heist from the Cloud

PayPal Ups Its Digital Resiliency

Bulgaria: A Whole Nation Hacked

VIDEO CASES

Stuxnet and Cyberwarfare

Cyberespionage: The Chinese Threat

Instructional Videos:

Sony PlayStation Hacked; Data Stolen from 77 Million Users

Meet the Hackers: Anonymous Statement on Hacking Sony

MyLab MIS

Discussion Questions: 8-5, 8-6, 8-7; **Hands-On MIS Projects**: 8-8, 8-9, 8-10, 8-11;
eText with Conceptual Animations

Cyberattacks in the Asia-Pacific Target the Weakest Link: People

Since the Asia-Pacific (APAC) region's focus on IT and the Internet has increased, it has become the next big target for cyberattacks. Geopolitical tensions and relatively weaker cyber regulations in the APAC region have further increased the risk of cyber exploitation.

Countries like Singapore are much more vulnerable than most other Asian countries because technology is so pervasive—forming, as it were, the country's digital lifeline. For example, in August 2017, hackers targeted Singapore Airlines (SIA), emailing the company's customers prior to its 70th anniversary and promising free tickets and prizes if they responded to survey questions. These attacks mimicked SIA's communications patterns and were personalized to include even the customer's frequent-flyer category. The emails were so legitimate-seeming that many customers had no worries at all about divulging their personal data. The attackers also replied to phone calls using the modified caller IDs of SIA's official telephone numbers. Additionally, a fake website resembling the official one was created to further gain the confidence of consumers.

Such attacks, called phishing, have become prevalent in Singapore, with as many as four in ten Singapore executives having fallen prey to them. In this case, SIA acted quickly in response, turning to traditional as well as social media to warn its customers. It also created a feedback page on its official website to advise customers about the authenticity of emails purportedly from SIA.

The banking industry has also been a key target of phishing, and one of its more prominent victims was the Overseas Chinese Banking Corporation (OCBC), which had earned plaudits for its exceptional management in Singapore and the Asia-Pacific. OCBC was targeted using both a phishing website and phone phishing, and over a two-week period received a total of 1,081 complaints about phone calls made by attackers impersonating the bank. The call would typically start with an automated voice message requesting a response, following which it would be transferred to a Mandarin-speaking person of non-local origin who would ask for sensitive information like personal and banking details. The OCBC now issues warnings to its customers and offers a security guarantee whereby victims of online fraud are guaranteed a full refund (subject to terms and conditions).

In July 2018, the government of Singapore revealed that hackers had broken into the nation's healthcare system and stole 1.5 million health records, including those of the prime minister. Authorities believe the attack was state-sponsored and very professional. Between December 2018 and June 2019, there were eight waves of cyberattacks across Southeast Asia, launched against governments, embassies,

© Andriy Popov/123RF

and organizations with government links. The attacks included the circulation of fake government documents and press releases, attached to which were malware designed to compromise the security of the unwitting recipient. Cybersecurity experts have linked the attacks to a cyber espionage group named Rancor.

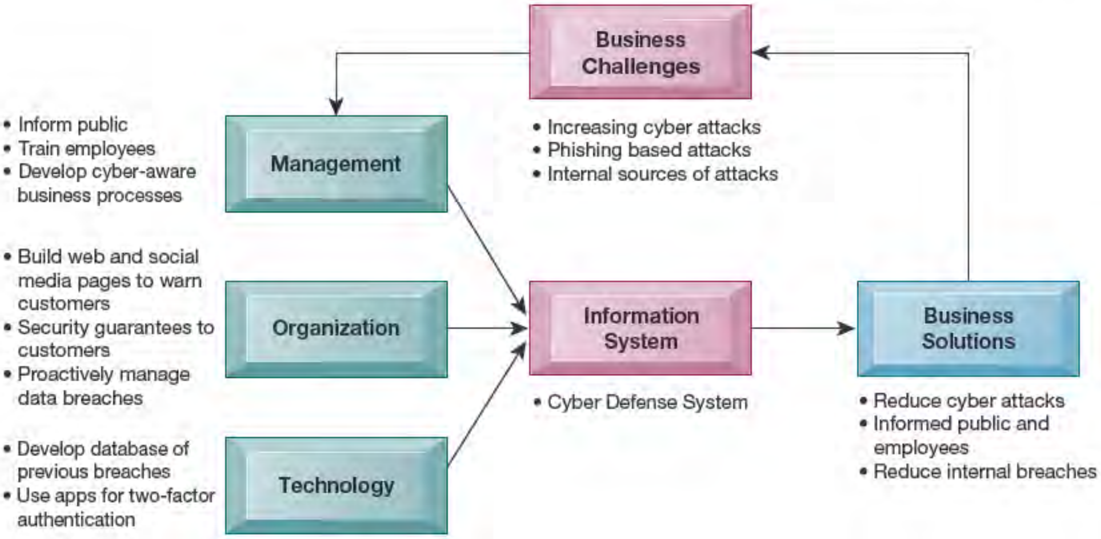
Attacks from external sources such as the above are often the most visible, but a majority of the data leaks in Asia—as high as 56 percent—are from internal sources, including company staff and executives. One of the reasons is that many Asian companies are highly networked and deal with numerous external partners. For example, several Development Bank of Singapore (DBS) employees in Hong Kong were arrested for an alleged leak of customer data. The staff had purportedly bribed department managers for customers' data, which they passed on to call centers in mainland China. These call centers would try to persuade customers to accept bank loans, and the commissions were shared with the DBS staff. Suspicion arose when many customers complained about receiving marketing calls from DBS, and the monthly sales of some of the DBS staff were found to exceed HK$1 million (S$183,870).

According to a report by Kaspersky Lab, there were 1.6 million cyberattacks on small and medium-sized enterprises in Southeast Asia in the first six months of 2020. Vietnam suffered the highest number of attacks with 464,300 cases, a 39 percent increase from 2019. One of the main reasons cited for the massive increase in such attacks was cybercriminals trying to take advantage of the greater number of employees working from home and thereby following less stringent protocols.

Sources: Janet Dang, "Vietnam among Top of Cyberattack in South East Asia," *Vietnam Times*, August 29, 2020; Ravie Lakshmanan, "Chinese Hacking Group Targets Southeast Asian Governments with Data-stealing Malware," TNW, October 2, 2019, thenextweb.com; Adrian Wan, "New UN Tool Maps Asia-Pacific Cybersecurity Landscape," Internet Society, January 29, 2019; Aaron Tan, "APAC Cyber Security Landscape to Become More Tumultuous in 2019" computerweekly.com, December 19, 2018; Matthew Field, "Cyber Attack on Singapore Health Database Steals Details of 1.5m Including Prime Minister," *The Telegraph*, July 20, 2018; S. Barker, "Employees, C-level & IT staff behind More Than Half of ASEAN Data Leaks," securitybrief.asia, October 24, 2017; L. Lam, "Singapore Airlines Giving Away Free Tickets? It's a Phishing Scam, SIA Warns," straitstimes.com, August 26, 2017; Channel NewsAsia, "Beware of Emails, Calls Claiming Singapore Airlines Is Giving Away Free Tickets: SIA," channelnewsasia.com, August 26 2017; PwC, Global State of Information Security® Survey 2017, Singapore, pwc.com, 2017; G. Aaron and R. Rasmussen, Global Phishing Survey: Trends and Domain Name Use in 2016, Anti Phishing Working Group, docs.apwg.org, June 26, 2017; I. Tham, "Singtel Vendor Fined $10k for Data Breach," straitstimes.com, April 18, 2017; "Sharp Rise in Phone Scams Impersonating OCBC, Says Bank," straitstimes.com, July 18, 2016; E. Estopace, "Asia-Pacific's 'Cyber Five' Nations More Vulnerable to Cyberattack," www.enterpriseinnovation.net, February 29, 2016.

Case contributed by Neerja Sethi and Vijay Sethi, Nanyang Technological University

Information systems security can be compromised in many ways, as illustrated by the examples in the opening case. Protecting systems through technical means—firewalls, intrusion detection systems, etc.—is necessary but not sufficient by itself. From employees within the organization to customers without, people are vital cogs in the security wheel, which rests on many different pillars, as shown in the opening diagram. It also involves designing robust business processes and monitoring them, as the DBS case demonstrated, where unusually high sales numbers led to the detection of a data breach.


Business Challenges
• Increasing cyber attacks
• Phishing based attacks
• Internal sources of attacks
Management
• Inform public
• Train employees
• Develop cyber-aware business processes
Organization
• Build web and social media pages to warn customers
• Security guarantees to customers
• Proactively manage data breaches
Technology
• Develop database of previous breaches
• Use apps for two-factor authentication
Information System
• Cyber Defense System
Business Solutions
• Reduce cyber attacks
• Informed public and employees
• Reduce internal breaches

Here are some questions to think about: What security vulnerabilities were exploited by hackers? What management, organizational, and technological factors contributed to these security weaknesses? What was the business impact of these problems? How important are ethics and morals to information systems security?

8-1 Why are information systems vulnerable to destruction, error, 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 within 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 was destroyed or divulged, your business might never be able to recover!

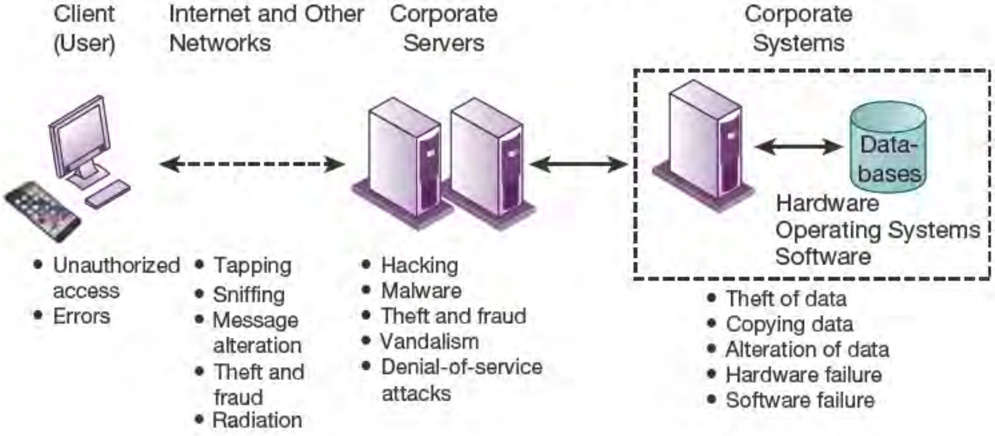
In short, if you operate a business today, you need to make security and control a top priority. **Security** refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems. **Controls** are methods, policies, 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 kinds of threats. Through communications networks, information systems in different locations are interconnected. The potential for unauthorized access or damage is not limited to a single location but can occur at many access points in the network. Figure 8.1 illustrates the most common threats

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.



against contemporary information systems. They can stem from technical, organizational, and environmental factors compounded by poor management decisions. In the multitier client/server computing environment illustrated here, vulnerabilities exist at each layer and in the communications between the layers. Users at the client layer can cause harm by introducing errors or by accessing systems without authorization. It is possible to access data flowing over networks, steal valuable data during transmission, or alter data 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 websites. Those capable of penetrating corporate systems can steal, 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 contributes to system vulnerability if valuable information resides on networks and computers outside the organization's control. Without strong safeguards, valuable data could be lost, be destroyed, or fall into the wrong hands, revealing important trade secrets or information that violates personal privacy.

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 that corporate employees use often contain sensitive data such as sales figures, customer names, phone numbers, and email addresses. Intruders may also 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 links to the corporate network, the organization's information systems are even more vulnerable to actions from outsiders.

Vulnerability has also increased from widespread use of email, instant messaging (IM), and peer-to-peer (P2P) file-sharing programs. Email may contain attachments that serve as springboards for malicious software or unauthorized access to internal corporate systems. Employees may use email messages to transmit valuable trade secrets, financial data, or confidential customer information to unauthorized recipients. Instant messaging activity over the Internet can in some cases be used as a back door to an otherwise secure network. Sharing files over P2P networks, such as those for illegal music sharing, can also transmit malicious software or expose information on either individual or corporate computers to outsiders.

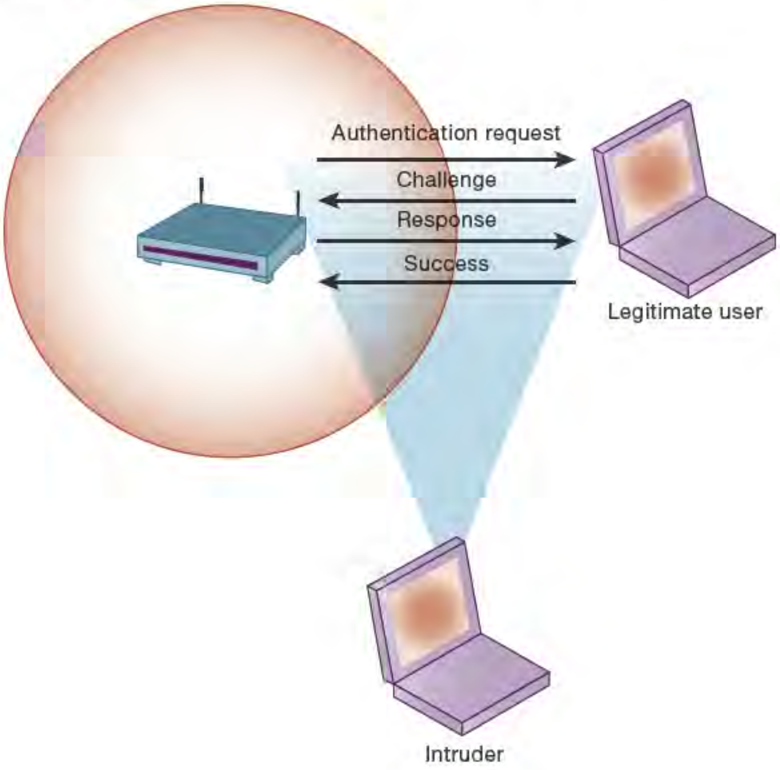
Wireless Security Challenges

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**,

FIGURE 8.2 WI-FI SECURITY CHALLENGES

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



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

An intruder who 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.

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. (See Table 8.1.) A **computer virus** is a rogue software program that attaches itself to other software programs or data files 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 email attachment or copying an infected file.

Worms 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 to spread rapidly from computer to computer. 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 email transmissions; or from compromised email messages, online ads, or instant messaging. Viruses have also invaded computerized information systems from infected external storage devices or infected machines. Especially prevalent today are **drive-by downloads**,

TABLE 8.1 EXAMPLES OF MALICIOUS CODE

NAME	TYPE	DESCRIPTION
Cryptolocker	Ransomware/ Trojan	Hijacks users' photos, videos, and text documents; encrypts them with virtually unbreakable asymmetric encryption; and demands ransom payment for them.
Conficker	Worm	First detected in November 2008 and still a problem. Uses flaws in Windows software to take over machines and link them into a virtual computer that can be commanded remotely. Had nearly 10 million computers worldwide under its control. Difficult to eradicate.
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 and caused an estimated $14.8 billion to $18.6 billion in damages.
ILOVEYOU	Virus	First detected on May 3, 2000. Script virus written in Visual Basic script and transmitted as an attachment to email 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.

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-connected 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 to a robot in a botnet to send email and text messages to anyone. According to IT security experts, mobile devices now pose the greatest security risks, outpacing those from larger computers. Kaspersky Lab reported there were 116.5 million malicious mobile malware attacks in 2018, double the number of the previous year (Kaspersky Lab, 2019).

Android, which is the world's leading mobile operating system, is the mobile platform targeted by most hackers. 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, Twitter, and LinkedIn have emerged as new conduits for malware. Members are more likely to trust messages they receive from friends, even if this communication is not legitimate. For example, the Facebook Messenger virus is caused by phishing messages sent from a hijacked Facebook account. Malicious spam messages are sent to everybody in the victim's Facebook contact list (2-Spyware, 2020).

The Internet of Things (IoT) introduces additional security challenges from the Internet-linked devices themselves, their platforms and operating systems, their communications, and even the systems to which they're connected. New security tools will be required to protect IoT devices and platforms from both information attacks and physical tampering, to encrypt their communications, and to address new challenges such as attacks that drain batteries. Many IoT devices such as sensors have simple processors and operating systems that may not support sophisticated security approaches.

Many malware infections are Trojan horses. 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 wooden horse the Greeks used to trick the Trojans into opening the gates to their fortified city during the Trojan War.

An example of a modern-day Trojan horse is the ZeuS (Zbot) Trojan, which infected more than 3.6 million computers in 2009 and still poses a threat. It has been used to steal login credentials for banking by surreptitiously capturing people's keystrokes as they use their computers. Zeus is spread mainly through drive-by downloads and phishing, and recent variants have been difficult to eradicate.

SQL injection attacks exploit 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 validate properly or filter data a user enters 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. Malware known as **ransomware** is proliferating on both desktop and mobile devices. Ransomware tries to extort money from users by taking control of their computers, blocking access to files, or displaying annoying pop-up messages. For example, in 2019, twenty-two Texas cities were held hostage for millions of dollars after ransomware called Sodinokibi infiltrated their computer systems and encrypted their data (Fruhlinger 2020). You can get ransomware from downloading an infected attachment, clicking a link inside an email, or visiting the wrong website.

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 an infringement on their 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 email accounts, to obtain passwords to protected computer systems, or to pick up personal information such as credit card or bank account numbers. The Zeus Trojan described earlier uses keylogging. Other spyware programs reset web browser home pages, redirect search requests, or slow performance by taking up too much computer resources.

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 gain unauthorized access by finding weaknesses in the security protections websites and computer systems employ. 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 website or corporate information system.

Spoofing and Sniffing

Hackers attempting to hide their true identities often spoof, or misrepresent, themselves by using fake email addresses or masquerading as someone else. **Spoofing** may also 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 website 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 will provide more detail about 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 email 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 many launch points.

Although DoS attacks do not destroy information or access restricted areas of a company's information systems, they often cause a website 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 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 to the infected computer. When hackers infect enough computers, they can use the amassed resources of the botnet to launch DDoS attacks, phishing campaigns, or unsolicited spam email.

Ninety percent of the world's spam and 80 percent of the world's malware are delivered by botnets. A recent example is the Mirai botnet, which infected numerous IoT devices (such as Internet-connected surveillance cameras) in October 2016 and then used them to launch a DDoS attack against Dyn, whose servers monitor and reroute Internet traffic. The Mirai botnet overwhelmed the Dyn servers, taking down Etsy, GitHub, Netflix, Shopify, SoundCloud, Spotify, Twitter, and a number of other major websites. A Mirai botnet variant attacked financial firms in January 2018, and Mirai variants are still active.

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. 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 computer crime—how many systems are invaded, how many people engage in the practice, or the total economic damage. According to Accenture and the Ponemon Institute's Ninth Annual Cost of Cyber Crime Study, the average annualized cost of cybercrime security for benchmarked organizations was U.S. $13 million in 2018 (Accenture, 2019).

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 email or messaging for threats or harassment
Intentionally attempting to intercept electronic communication
Illegally accessing stored electronic communications, including email and voice mail
Transmitting or possessing child pornography by using a computer

Many companies are reluctant to report computer crimes because the crimes may involve employees or that publicizing vulnerability will hurt their reputations. The most economically damaging kinds of computer crime are DoS attacks, activities of malicious insiders, and web-based attacks.

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 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. Identity theft has flourished on the Internet, with credit card files a major target of website hackers. According to the 2020 Identity Fraud Study by Javelin Strategy & Research, identity fraud losses in the United States reached $16.9 billion in 2019 (Javelin, 2020).

One popular tactic is a form of spoofing called **phishing**. Phishing involves setting up fake websites or sending email messages that look like those of legitimate businesses to ask users for confidential personal data. The email 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 email message, by entering the information at a bogus website, or by calling a telephone number. eBay, PayPal, Amazon.com, Walmart, and a variety of banks have been 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 Internet service providers (ISPs) store to speed up web browsing and flawed software on ISP servers allows the fraudsters to hack in and change those addresses.

According to the Ponemon Institute and IBM Security's 2019 Cost of a Data Breach Report, the total average cost of a data breach among the 507 companies surveyed globally was $3.92 million (Ponemon, 2019). Moreover, brand damage can be significant although hard to quantify. In addition to the data breaches described in case studies for this chapter, Table 8.3 describes other major data breaches.

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 websites federal crimes.

U.S. legislation, such as the Wiretap Act, Wire Fraud Act, Economic Espionage Act, Electronic Communications Privacy Act, CAN-SPAM Act, and Protect Act of 2003, covers computer crimes involving intercepting electronic

TABLE 8.3 MAJOR DATA BREACHES

DATA BREACH	DESCRIPTION
Marriott	In November 2018, the world's largest hotel company revealed that a hack in the reservation database for its Starwood properties may have exposed the personal information of up to 500 million guests. Exposed data included names, phone numbers, email addresses, passport numbers, date of birth, and credit card numbers. State-sponsored Chineae hackers copied and encrypted data, and took steps toward removing them. In March 2020, Marriott was hacked again after the login credentials of 2 employees were used.
Yahoo	In September and December 2016, Yahoo disclosed that it had been the target of two of the biggest data breaches ever, with sensitive information stolen from more than 1 billion user accounts in 2013 and 500 million in 2014. State-sponsored hackers found a way to forge credentials to log into some users' accounts without a password. These data breaches forced Yahoo to lower its selling price by $300 million when it was acquired by Verizon in June 2017. In October 2017, Verizon reported that every single Yahoo account had actually been hacked—3 billion accounts, including email, Tumblr, Flickr, and Fantasy.
Danish Tax Administration	A software error in the Danish tax administrations self-service tax portal accidentally exposed the personal identification numbers for 1.26 million Danish citizens, a fifth of the country's total population. The leak was discovered in January 2020 and had gone undetected for 5 years. Every time a user updated account details in the portal's settings section, their personal identification number would be added to the URL, which would then be collected by analytics services running on the site -- in this case, Adobe and Google.
EasyJet	UK budget airline EasyJet announced on May 19, 2020 that a cyberattack may have exposed information belonging to 9 million customers, including over 2,200 credit card records with CVV numbers. The sensitive personal data leaked included full names, email addresses, and travel data that specified departure dates, arrival dates, and booking dates. EasyJet is facing an £18 billion class-action lawsuit filed on behalf of customers impacted by the data breach..

communication, using electronic communication to defraud, stealing trade secrets, illegally accessing stored electronic communications, using email for threats or harassment, and transmitting or possessing child pornography. All 50 U.S. states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches involving personally identifiable information.

Click Fraud

When you click 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 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 websites that feature pay-per-click online advertising.

Some companies hire third parties (typically from low-wage countries) to click a competitor's ads fraudulently 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 and have made some changes to curb it.

Global Threats: Cyberterrorism and Cyberwarfare

The cyber criminal activities we have described—launching malware, DoS attacks, and phishing probes—are borderless. Attack servers for malware are now hosted in more than 200 countries and territories. The leading sources of malware attacks include the United States, China, Brazil, India, Germany, and Russia. 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 to cause damage and disruption. Examples include efforts of Russian hackers to disrupt U.S. 2016 presidential elections and to penetrate the U.S. power grid. Cyberwarfare also includes defending against these types of attacks.

Cyberwarfare is more complex than conventional warfare. Although many potential targets are military, a country's power grids, dams, financial systems, communications networks, and voting systems can also be crippled. Nonstate actors such as terrorists or criminal groups can mount attacks, and it is often difficult to tell who is responsible. Nations must constantly be on the alert for new malware and other technologies that could be used against them, and some of these technologies developed by skilled hacker groups are openly for sale to interested governments.

Cyberwarfare attacks have become much more widespread, sophisticated, and potentially devastating. Foreign hackers have stolen source code and blueprints to the oil and water pipelines and power grid of the United States and infiltrated the Department of Energy's networks hundreds of times. Over the years, hackers have stolen plans for missile tracking systems, satellite navigation devices, surveillance drones, and leading-edge jet fighters.

According to U.S. intelligence, more than 30 countries are developing offensive cyberattack capabilities, including Russia, China, Iran, and North Korea. Their cyberarsenals include collections of malware for penetrating industrial, military, and critical civilian infrastructure controllers; email lists and text for phishing attacks on important targets; and algorithms for DoS attacks. U.S. cyberwarfare efforts are concentrated in the United States Cyber Command, which coordinates and directs the operations and defense of Department of Defense information networks and prepares for military cyberspace operations. 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.

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. 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 coworkers 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**.

Insiders bent on harm have also exploited their knowledge of the company to break into corporate systems, including those running in the cloud. The Interactive Session on Technology shows how a former employee at Amazon Web Services used her knowledge of Amazon cloud security to steal many millions of Capital One Financial customer records stored by Amazon's cloud computing service.

INTERACTIVE SESSION TECHNOLOGY

Capital One: A Big Bank Heist from the Cloud

Capital One Financial Corporation is an American bank holding company specializing in credit cards, auto loans, banking, and savings accounts. It is the eleventh largest bank in the United States in terms of assets and an aggressive user of information technology to drive its business. Capital One was an early adopter of cloud computing and a major client of Amazon Web Services (AWS). Capital One has been trying to move more critical parts of its IT infrastructure to Amazon's cloud infrastructure in order to focus on building consumer applications and other needs.

On July 29, 2019, Capital One and its customers received some very bad news. Capital One had been breached, exposing over 140,000 Social Security numbers, 80,000 bank account numbers, tens of millions of credit card applications, and one million Canadian social insurance numbers (equivalent to Social Security numbers in the US). It was one of the largest thefts of data ever from a bank.

The culprit turned out to be Paige Thompson, a former employee of Amazon Web Services, which hosted the Capital One database that was breached. Thompson was arrested in Seattle and charged with one count of computer fraud and abuse. She had worked for the same server business that court papers said Capital One was using. Thompson could face up to five years in prison and a $250,000 fine.

The bank believed it was unlikely that Thompson disseminated the information or used it for fraud. But it will still cost the bank up to $150 million, including paying for credit monitoring of affected customers.

Amazon Web Services hosts remote servers that organizations use to store their data. Large enterprises such as Capital One build their own web applications using Amazon's cloud servers and data storage services data so they can use the information for their specific needs.

The F.B.I. agent investigating the breach reported that Ms. Thompson had gained access to Capital One's sensitive data through a "misconfiguration" of a firewall on a web application. (A firewall monitors incoming and outgoing network traffic and blocks unauthorized access.) This allowed her to communicate with the server where Capital One was storing its data and customer files. Capital One stated it had immediately fixed the configuration vulnerability once it had been detected. Amazon said its customers fully control the applications they build and that it had found no evidence that its underlying cloud services had been compromised.

Thompson was able to access and steal this sensitive information only because Capital One had misconfigured its Amazon server. Thompson could then trick a system in the cloud to uncover the credentials she needed to access Capital One's customer records. Thompson's crime was considered an insider threat, since she had worked at Amazon years earlier. However, outsiders also try to search for and exploit this type of misconfiguration, and server misconfigurations are commonplace. Misconfigurations are also easily fixed, so many do not consider them a breach. Sometimes it's difficult to determine whether tinkering with misconfigurations represents a criminal activity or security research.

Thompson was able to tap into Amazon's metadata service, which has the credentials and other data required to manage servers in the cloud. Ms. Thompson ran a scan of the Internet to identify vulnerable computers that could provide access to a company's internal networks. She found a computer managing communications between Capital One's cloud and the public Internet that had been misconfigured, with weak security settings. Through that opening Thompson was able to request the credentials required to find and read Capital One data stored in the cloud from the metadata service. Once Thompson located the Capital One data, she was able to download them without triggering any alerts. Thompson also boasted online that she had used the same techniques to access large amounts of online data from other organizations.

Amazon has stated that none of its services, including the metadata service, were the cause of the break-in and that AWS offers monitoring tools for detecting this type of incident. It is unclear why none of these alerting tools triggered an alarm when Thompson was hacking into Capital One. Thompson began hacking Capital One on

March 12, 2019, but went undetected until an outside researcher tipped off Capital One 127 days later. According to C. J. Moses, deputy chief information security officer for AWS, Amazon restricts most staff members from accessing its broader internal infrastructure in order to protect against "witting or unwitting" data breaches.

Security professionals have known about misconfiguration problems and the ability to steal credentials from the metadata service since at least 2014. Amazon believes it is the customer's responsibility to solve them. Some customers have failed to do so. When security researcher Brenton Thomas conducted an Internet scan in February 2019, he found more than 800 Amazon accounts that allowed similar access to the metadata service. (Amazon's cloud computing service has over one million users.) But Thomas also found other cloud computing companies with misconfigured services as well, including Microsoft's Azure cloud.

Whatever the cloud service, the pool of talent capable of launching similar attacks is expanding. Given the nature of cloud services, any person who has worked on developing technology at any of the major cloud computing companies can learn how these systems work in practice.

Capital One had a reputation for strong cloud security. The bank had conducted extensive due diligence before deciding to move to cloud computing in 2015. However, before the giant data breach, Capital One employees had raised concerns internally about high turnover in the company's cybersecurity unit and tardiness in installing some software to help spot and defend against hacks. The cybersecurity unit is responsible for ensuring Capital One's firewalls are properly configured and for scanning the Internet for evidence of a data breach. In recent years there have been many changes among senior leaders and staffers. About a third of Capital One's cybersecurity employees left the company in 2018.

Sources: Robert McMillan, "How the Accused Capital One Hacker Stole Reams of Data from the Cloud," *Wall Street* Journal, August 4, 2019; Emily Flitter and Karen Weiser, "Capital One Data Breach Compromises Data of Over 100 Million," *New York Times,* July 29, 2019; James Randle and Catherine Stupp, "Capital One Breach Highlights Dangers of Insider Threats," *Wall Street Journal*, July 31, 2019. Peter Rudegeair, AnnaMaria Andriotis, and David Benoit, "Capital One Hack Hits the Reputation of a Tech-Savvy Bank," *Wall Street Journal*, July 31, 2019.

CASE STUDY QUESTIONS

1. What management, organization, and technology factors were responsible for the Capital One hack?
2. Was this an insider hack? Explain your answer.
3. What steps could have been taken to prevent the Capital One hack?
4. Should companies handling sensitive data use cloud computing services? Explain your answer.

Software Vulnerability

Software errors pose a constant threat to information systems, causing untold losses in productivity and sometimes endangering people who use or depend on systems. Growing complexity and size of software programs, coupled with demands for rapid delivery to markets, have contributed to an increase in software flaws or vulnerabilities.

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 paths. Important programs within most corporations are usually much larger, containing tens of thousands or even millions of lines of code, each with many times the choices and paths of the smaller programs.

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

Flaws in commercial software not only impede performance but also create security vulnerabilities that open networks to intruders. Each year security firms identify thousands of software vulnerabilities in Internet and PC software. For example, in May 2019 Facebook had to fix a flaw in its WhatsApp encrypted-messsaging app that allowed attackers to install spyware on mobile phones (McMillan, 2019). Especially troublesome are **zero-day vulnerabilities**, which are holes in the software unknown to its creator. Hackers then exploit this security hole before the vendor becomes aware of the problem and hurries to fix it. This type of vulnerability is called *zero-day* because the author of the software has zero days after learning about it to patch the code before it can be exploited in an attack. Sometimes security researchers spot the software holes, but more often, they remain undetected until an attack has occurred.

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. 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 a company uses 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.

Newly Discovered Vulnerabilities in Microprocessor Design

Recently discovered vulnerabilities such as Spectre and Meltdown stem from flaws in the design of computer microprocessor chips, which enable hackers using malicious software programs to gain access to data that were thought to be completely protected. These vulnerabilities affect nearly every computer chip manufactured in the last 20 years. Major software vendors have rolled out workaround patches, but the only way to truly fix Meltdown and Spectre is to replace the affected processors.

8-2 What is the business value of security and control?

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 weapon 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 have permanent impacts on 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.

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, U.S. retailer Target had to pay $39 million to several U.S. banks servicing Mastercard that were forced to reimburse Target customers millions of dollars when those customers lost money due to a massive 2013 hack of Target's payment systems affecting 40 million people. Target also paid $67 million to Visa for the data hack and $10 million to settle a class-action lawsuit brought by Target customers. Developing a sound security and control framework that protects business information assets is of critical importance to the entire enterprise, including senior management. It can no longer be limited to the IT department (Rothrock et al., 2018).

Legal and Regulatory Requirements for Electronic Records Management

Government regulations worldwide 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, such as the General Data Protection Regulation (GDPR) in the EU (see Chapter 4), for the retention and storage of electronic records as well as for privacy protection.

In the U.S., regulations of this type tend to be industry-specific. For instance, the Health Insurance Portability and Accountability Act (**HIPAA**) of 1996 outlines security and privacy rules and procedures for simplifying the administration of healthcare billing and automating the transfer of healthcare data between healthcare providers, payers, and plans. It specifies privacy, security, and electronic transaction standards for healthcare providers handling patient information, requires the retention of patient information for six years, and provides penalties for breaches of medical privacy, disclosure of patient records by email, or unauthorized network access. In the UK, the Records Management Code of Practice for Health and Social Care 2020 supplements the GDPR with specific regulations for managing such records (NHS, 2020).

The U.S. Financial Services Modernization Act of 1999, better known as the **Gramm-Leach-Bliley 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.

The U.S. Public Company Accounting Reform and Investor Protection Act of 2002, better known as the **Sarbanes-Oxley Act**, is designed to protect investors in 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. In the UK, the Companies Act 2006, the UK Corporate Governance Code, and UK listings rules for public companies impose similar requirements (Hinks, 2020).

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 and computer hard disk drives as well as in email, text messages, and e-commerce transactions over the Internet.

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, email, 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 often 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 What are the components of an organizational 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 the systems development process, 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. You can find more detail about application and general controls in our Learning Tracks.

Information systems controls should not be an afterthought. They need to be incorporated into the design of a system and should consider not only how the system will perform under all possible conditions but also the behavior of organizations and people using the system.

TABLE 8.4 GENERAL CONTROLS

TYPE OF GENERAL CONTROL	DESCRIPTION
Software controls	Monitor the use of system software and prevent unauthorized access and use 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 maintained internally or by an external hosting service 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.

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

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 $1000 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 and dividing by two. The expected annual loss for each exposure can be determined by multiplying the average loss by its probability of occurrence.

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

After 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

After 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-years disaster? Management must estimate how much it will cost to achieve this level of acceptable risk.

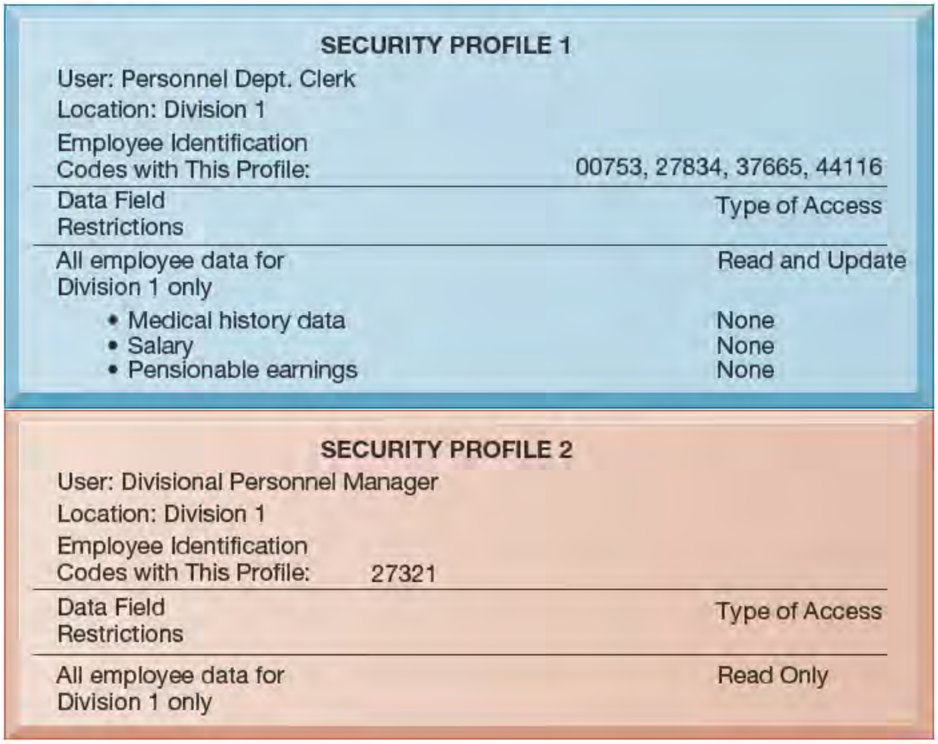
The security policy drives other policies determining acceptable use of the firm's information resources and which members of the company have access to its information assets. An **acceptable use policy (AUP)** defines acceptable uses of the firm's information resources and computing equipment, including desktop and laptop computers, mobile devices, telephones, and the Internet. A good AUP defines unacceptable and acceptable actions for every user and specifies consequences for noncompliance.

Figure 8.3 is one example of how an organization might specify 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

FIGURE 8.3 **ACCESS RULES FOR A PERSONNEL SYSTEM**

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.



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

for his or her division, including medical history and salary. We provide more detail about 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 disrupted computing and communications services. 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 cloud-based disaster recovery services or firms such as SunGard Availability Services that provide sites with spare computers around the country where subscribing firms can run their critical applications in an emergency.

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. PricewaterhouseCoopers LLP (PwC) UK has developed business continuity plans to provide resilient and recoverable operations to service its clients in the event of crises such as the collapse of a key supplier, employees off sick in a pandemic, or the failure of a critical system shutting down services. There are continuity plans for how PwC uses technology, operates engagement teams, and utilizes internal PwC services. PwC designed the most important aspects of how it delivers client service to be fault tolerant, minimizing any single-points-of-failure.

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

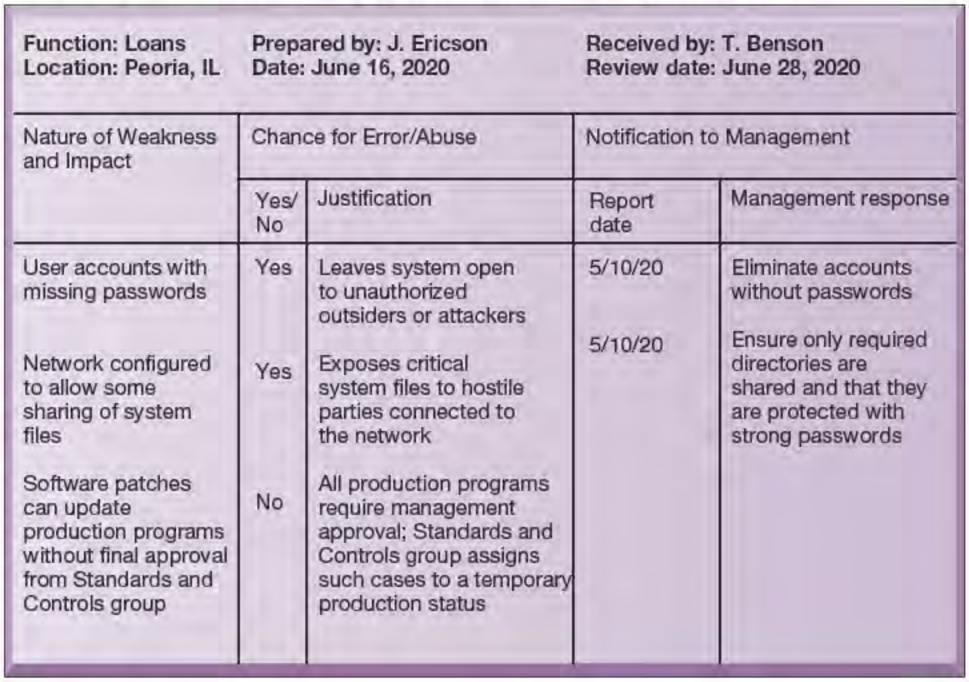
How does management know that information systems security and controls are effective? To answer this question, organizations must conduct comprehensive and systematic audits. An **information systems audit** examines the firm's overall security environment as well as controls governing individual information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

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

The audit lists and ranks all control weaknesses and estimates the probability of their occurrence. It then assesses the financial and organizational impact of each threat. Figure 8.4 is a sample auditor's listing of control weaknesses for

FIGURE 8.4 SAMPLE AUDITOR'S LIST OF CONTROL WEAKNESSES

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 management takes.



Function: Loans **Location: Peoria, IL**	**Prepared by: J. Ericson** **Date: June 16, 2020**	**Received by: T. Benson** **Review date: June 28, 2020**

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	5/10/20	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	5/10/20	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		

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 What are the most important tools and technologies for safeguarding 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 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 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, voice, or retinal image, against a stored profile of these characteristics to determine 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 (and some smartphones) equipped with fingerprint identification devices and some models with built-in webcams and face recognition software. Financial service firms such as Vanguard and Fidelity have implemented voice authentication systems for their clients.

The steady stream of incidents in which hackers have been able to access traditional passwords highlights the need for more secure means of authentication. **Two-factor authentication** increases security by validating users through

© Anyaberkut/123RF

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

a multistep process. To be authenticated, a user must provide two means of identification, one of which is often a physical token, such as a smartcard or chip-enabled bank card, and the other of which is typically data, such as a password or personal identification number (PIN). Biometric data, such as fingerprints, iris prints, or voice prints, can also be used as one of the authenticating mechanisms. A common example of two-factor authentication is a bank card; the card itself is the physical item, and the PIN is the other piece of data that goes with it.

Firewalls, Intrusion Detection Systems, and Anti-malware Software

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

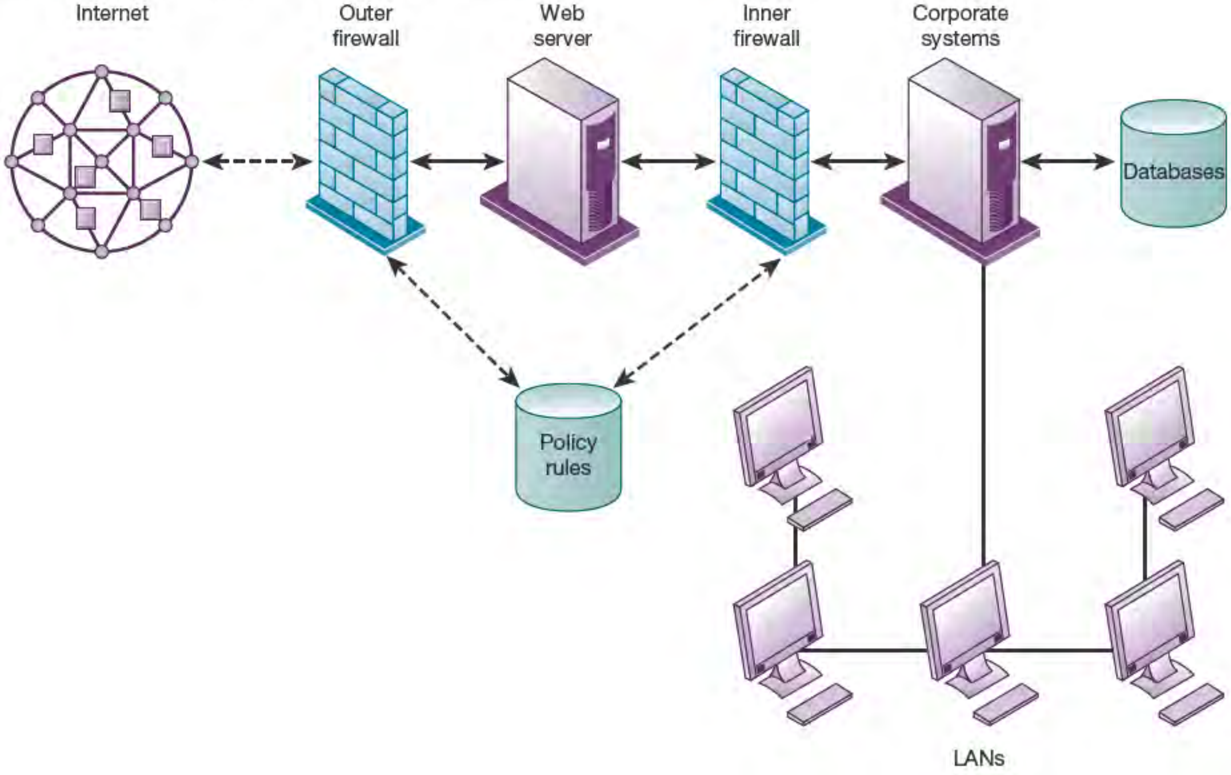
Firewalls

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 that examines each user's credentials before it grants access to a network. The firewall identifies names, IP addresses, applications, and other characteristics of incoming traffic. It checks this

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.



information against the access rules that the network administrator has programmed into the system. The firewall prevents unauthorized communication into and out of the network.

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

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 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 communicates with 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 whether important files have been removed or modified, and sends warnings of vandalism or system administration errors. The intrusion detection tool can also be customized to shut down a particularly sensitive part of a network if it receives unauthorized traffic.

Anti-malware Software

Defensive technology plans for both individuals and businesses must include anti-malware protection for every computer. **Anti-malware software** prevents, detects, and removes malware, including computer viruses, computer worms, Trojan horses, spyware, and adware. However, most anti-malware software is effective only against malware already known when the software was written. To remain effective, the software must be continually updated. Even then it is not always effective because some malware can evade detection. Organizations need to use additional malware detection tools for better protection.

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 anti-spam software. These comprehensive security management products are called **unified threat management (UTM)** systems. UTM products are available for all sizes of networks. Leading UTM vendors include Fortinent, Sophos, and Check Point, and networking vendors such as Cisco Systems and Juniper Networks provide some UTM capabilities in their products.

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. The most recent specification is WPA3, introduced in 2018.

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.

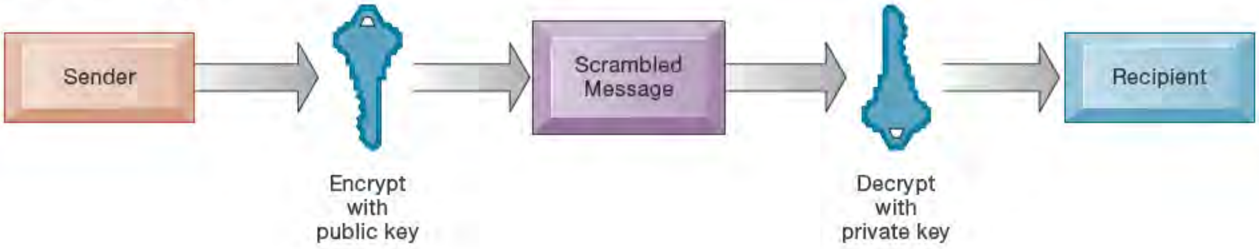
Two methods for encrypting network traffic on the web are SSL and S-HTTP. **Secure Sockets Layer (SSL)** and its successor, Transport Layer Security (TLS), enable client and server computers to manage encryption and decryption activities as they communicate with each other during a secure web session. **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.

Two methods of encryption are symmetric key encryption and public key encryption. In symmetric key encryption, the sender and receiver establish a

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 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.



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 56 to 256 bits long (a string of from 56 to 256 binary digits) depending on the level of security desired. The longer the key, the more difficult it is to break the key. The downside is that the longer the key, the more computing power it takes for legitimate users to process the information.

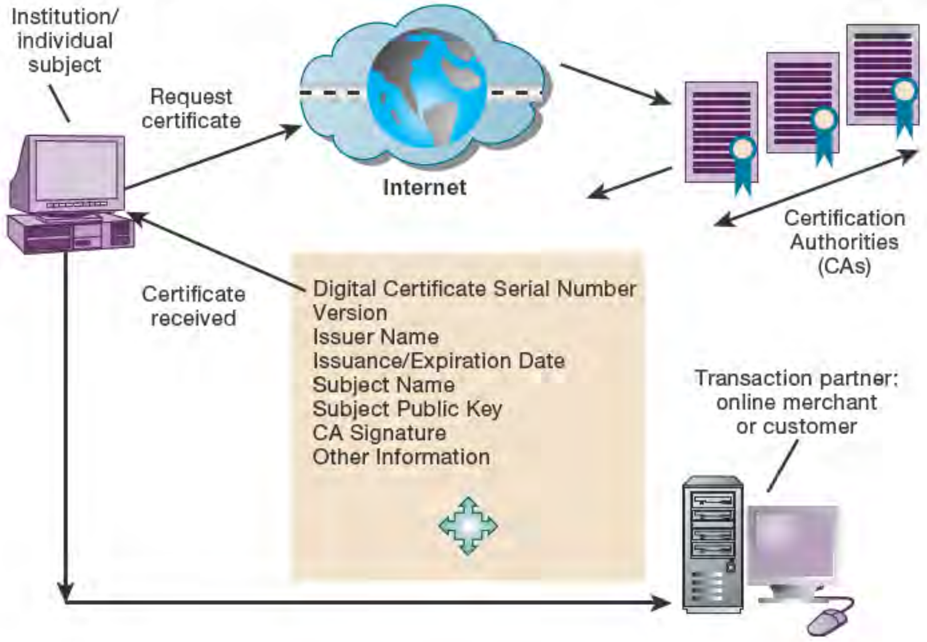
The problem with all symmetric encryption schemes is that the key itself must be shared somehow among the senders and receivers, which exposes the key to outsiders who might just be able to intercept and decrypt the key. A more secure form of encryption called **public key encryption** uses two keys: 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), 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. By 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.

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.



Securing Transactions with Blockchain

Blockchain, which we introduced in Chapter 6, is gaining attention as an alternative approach for securing transactions and establishing trust among multiple parties. A blockchain is a chain of digital "blocks" that contain records of transactions. Each block is connected to all the blocks before and after it, and the blockchains are continually updated and kept in sync. This makes it difficult to tamper with a single record because one would have to change the block containing that record as well as those linked to it to avoid detection.

Once recorded, a blockchain transaction cannot be changed. The records in a blockchain are secured through cryptography, and all transactions are encrypted. Blockchain network participants have their own private keys that are assigned to the transactions they create and act as a personal digital signature. If a record is altered, the signature will become invalid, and the blockchain network will know immediately that something is amiss. Because blockchains aren't contained in a central location, they don't have a single point of failure and cannot be changed from a single computer. Researchers point out, however, that blockchain is vulnerable in some of the same ways as conventional, centralized record-keeping systems. Blockchain systems still need careful attention to security and control as do other systems with high security requirements (Madnick, 2020).

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 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 or downtime. **Downtime** refers to periods of time in which a system is not operational.

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, AT&T, Verizon, IBM, Perimeter eSecurity, and Symantec are leading providers of MSSP services.

Achieving Digital Resiliency

Today's organizations are much more hypernetworked and interconnected than in the past, with important parts of their IT infrastructures maintained remotely in the cloud, managed by outsiders, and accessible by mobile devices. Firms are embracing the concept of **digital resiliency** to deal with the realities of this new digital environment. Digital resiliency deals with how to maintain and increase the resilience of an organization and its business processes in an all-pervasive digital environment, not just the resiliency of the IT function. In addition to computing, storage, and networking technologies, digital resiliency calls attention to managerial and organizational issues such as corporate policies and goals, business processes, organizational culture, business requirements, accountability, and business risk management. These factors can affect how well an organization can actually utilize and manage network connectivity, applications, databases, and data centers, its ability to provide 24/7 availability for business, and its ability to respond to changing business conditions. A single weak link in this chain can cause an outage or prevent the firm from responding to new challenges and opportunities, if resiliency has not been explicitly designed in, measured, and tested.

For example, many companies whose employees were required to work at home in the spring of 2020 to avoid exposure to the coronavirus were unsure of whether they had enough server capacity to support thousands more people working remotely. Had they used a digital resiliency approach, this contingency would have been better anticipated and planned for.

The Interactive Session on Management illustrates how PayPal, a heavily technology-driven business, was able to increase its digital resiliency by paying more attention to measuring the operational effectiveness of its data center teams and the reduction of employee errors.

INTERACTIVE SESSION MANAGEMENT

PayPal Ups Its Digital Resiliency

PayPal Holdings, Inc. is an American company operating a worldwide online payments system that supports online money transfers and serves as an electronic alternative to traditional payment methods like checks and money orders. The company operates as a payment processor for online vendors, auction sites, and many other commercial users. You've probably used PayPal if you've bought something from eBay or from an e-commerce website. It is a very well-established and widely accepted payment system. As of the first quarter of 2020, PayPal had 325 million active users. In 2019, PayPal processed 12.4 billion payment transactions and generated $17.77 billion in revenue.

Obviously this is a company that has to work vigilantly to make its services ultrasecure and available 24/7 throughout the world, and PayPal maintains very high standards of security and reliability. But management wanted to make sure the company was doing the best job possible, so it turned to Uptime Institute to evaluate the way PayPal ran its data centers and its level of digital resiliency. Uptime Institute is a consulting group focusing on improving the performance, efficiency, and reliability of business critical infrastructure through innovation, collaboration, and independent performance certifications.

Although data centers try to operate sites full of cost-saving technologies and innovative new approaches, they still struggle with the ongoing performance and reliability of these sites due to the operational plans in place. Various levels of staffing and experience along with limited or inaccurate written documentation of operational processes create inconsistent behaviors and service outages.

Uptime Institute had found that the majority of reported data center outages are directly related to human error. This could be operator error or management error in its decisions regarding staffing, maintenance, training, or overall rigor of operation. With human error responsible for so many data center incidents, organizations need to take a more holistic approach to staffing, organizational practices, maintenance and operations activities, management, and planning.

Sean Tugwell, PayPal's Director of Data Center Architecture and Engineering, wanted to make sure his company had achieved a high level of digital resilience and 99.999 percent availability across all data centers. He also wanted to make sure the colos working with PayPal were sufficiently resilient as well. (A colocation data center, often referred to as a "colo," is a large data center facility that rents out rack space to other businesses for their servers or other computing equipment.)

Uptime Institute's M&O Assessment measures the operational effectiveness of the teams within a data center, focusing on five behaviors that should be proactive, practiced, and informed. These behaviors apply to staffing and organization, maintenance, training, planning, coordination and management, and operating conditions. In early 2018, PayPal received Uptime Institute's M&O Stamp of Approval for its PHX01 data center, earning a very high first-time score of 96.2 percent. Several other PayPal data centers received high first-time scores of 100 percent, further indicating that PayPal had a high level of data center sophistication and maturity.

PayPal also scored well in its implementation of the Service Now platform, which is used for improving procedural approval workflows, maintenance management for critical data center infrastructure, incident management, and space and power planning. One area where PayPal shined was its approach to staffing and organization. Its Facilities Operations group has at least three facilities technicians on site at all times, and these technicians undergo rigorous training to ensure they have comprehensive and in-depth knowledge of a variety of systems and equipment.

PayPal's Facilities Operations group is also responsible for preventive and corrective maintenance at a data center. The group creates and implements on-site maintenance standards and procedures to make sure data center maintenance work is successfully completed and documented. In this area, too PayPal scored very well—all its data centers had no items for deferred maintenance. PayPal's Preventive Maintenance Program helps the company keep equipment in like-new condition.

New hires at PayPal's Facility Operations Team are required to complete an initial training program before they are allowed to work on shift. PayPal also has a training program for vendors who will be performing on-site maintenance.

To promote effective planning, coordination, and management that will result in greater uptime, PayPal has developed various procedures and standards, which are available in its ServiceNow Knowledge Base. This helps promote consistency across all of PayPal's data centers, and also reduces the chance for human error at each site. PayPal's financial team creates, reviews, and tracks budgets to ensure the budget for each data center is appropriate for supporting the firm's business objectives.

Consistency has become even more important for PayPal as it uses more colocation companies to add to its computing capacity. PayPal was able to use the M&O Stamp of Approval program to evaluate its colocation data center vendors. New vendor contracts now require that a data center vendor achieve Uptime Institute's M&O Stamp of Approval and maintain that rating as long as PayPal is a customer.

A high priority for PayPal's Data Center Services Team is reducing business costs. Any data center downtime, whether from a company data center or colo, creates a loss to the business, in terms of number of transactions processed, customer service, and the time and resources required to solve the downtime problem. Uptime Institute's M&O Stamp of Approval promotes this goal, and also helps teams make sure that there are no surprises when new teams and operational practices are introduced to the company.

Given the critical importance of digital resiliency, in addition to its M&O Assessment, Uptime Institute has also recently introduced a Digital Resiliency Assessment program. This program specifically focuses on the resiliency of a firm's internal and cloud-based digital infrastructure, spanning its end users, networks, applications, databases, and data centers, to identify any weak links in the chain and validate the resiliency of the entire system.

Sources: Uptime Institute, "Digital Infrastructure Resiliency Assessment," and "PayPal,"www.uptimeinstitute.com, accessed March 24, 2020; Craig Smith, "Amazing PayPal Statistics and Facts (2020) by the Numbers," DMR, March 12, 2020; and investor.paypal.com, accessed March 23, 2020.

CASE STUDY QUESTIONS

1. Why is digital resiliency so important for a company such as PayPal?
2. How did PayPal benefit from measuring its digital resiliency? What issues did it address?
3. What is the role of management and organizational issues in making an organization's IT infrastructure more resilient?

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. Using the public cloud disrupts traditional cybersecurity models that many companies have built up over years. As companies make use of the public cloud, they need to revise their cybersecurity practices in order to consume public-cloud services in a way that enables them both to protect critical data and to fully exploit the speed and agility that these services provide.

Managing security and privacy for cloud services is similar to managing traditional IT infrastructures. However, the risks may be different because some, but not all, responsibilities shift to the cloud service provider. The category of cloud service (IaaS, PaaS, or SaaS) affects exactly how these responsibilities are shared. For IaaS, the provider typically supplies and is responsible for securing basic IT resources such as machines, storage systems, and networks. The cloud services customer is typically responsible for its operating system, applications, and corporate data placed into the cloud computing environment. This means that most of the responsibility for securing the applications and the corporate data falls on the customer.

Cloud service customers should carefully review their cloud services agreement with their cloud provider to make sure their applications and data hosted in cloud services are secured in accordance with their security and compliance policies. However, although many organizations know how to manage security for their own data center—they're unsure of exactly what they need to do when they shift computing work to the cloud. They need new tool sets and skill sets to manage cloud security from their end to configure and launch cloud instances, manage identity and access controls, update security controls to match configuration changes, and protect workloads and data. There's a misconception among many IT departments that whatever happens in the cloud is not their responsibility. It is essential to update security requirements developed for enterprise data centers to produce requirements suitable for the use of cloud services.

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.

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 restore your data completely, 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. The Cloud Security Alliance (CSA) has created industrywide standards for cloud security, specifying best practices to secure cloud computing.

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. Data loss prevention technology can identify where critical data are saved, who is accessing the data, how data are leaving the company, and where the data are going. 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. The organization's mobile security policy should forbid employees from using unsecured, consumer-based applications for transferring and storing corporate documents and files or sending such documents and files to oneself by email without encryption. Companies should encrypt communication whenever possible. All mobile device users should be required to use the password feature found in every smartphone.

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

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

Good testing begins before a software program is even written, by using a *walkthrough*—a review of a specification or design document by a small group of people carefully selected based on the skills needed for the particular objectives being tested. When developers start writing software programs, coding walkthroughs can also be used to review program code. However, code must be tested by computer runs. When errors are discovered, the source is found and eliminated through a process called *debugging*. You can find out more about the various stages of testing required to put an information system into operation in Chapter 13. Our Learning Tracks also contain descriptions of methodologies for developing software programs that contribute to software quality.

8-5 How will MIS help my career?

Here is how Chapter 8 and this book can help you find an entry-level job as an identity access and management support specialist.

The Company

Value Supermarkets, a major supermarket grocery store chain headquartered in the UK, is looking to fill an entry-level position for an identity access and management support specialist. The company has over 100 stores, more than 5,000 workers, and nearly a million monthly shoppers.

Position Description

The identity access and management support specialist will be responsible for monitoring the company's identity management system to ensure that the company is meeting its audit and compliance controls. This position reports to the company's security operations manager. Job responsibilities include:

- Performing data integrity testing of identity management system integrations with business applications.
- Integrating Windows Active Directory files with the identity management system.
- Maintaining information on system user roles and privileges.

Job Requirements

- Bachelor's degree
- Proficiency with computers
- Ability to multitask and work independently
- Attention to detail
- Strong time management skills
- Ability to communicate with both technical and nontechnical staff

Interview Questions

1. What do you know about authentication and identity management? Have you ever worked with identity management or other IT security systems? What did you do with this software?
2. Have you ever worked with Windows Active Directory? What exactly did you do with this software?
3. What knowledge and experience do you have with ensuring data integrity?
4. Can you give an example of a situation where you had to multitask and manage your time and how you handled it?
5. Can you tell us about the computer experience you've had? What software tools have you worked with?

Author Tips

1. Review the last two sections of this chapter, especially the discussions of identity management and authentication. Also review the Chapter 6 discussions of data integrity and data quality.
2. Use the web to find out more about identity management, data integrity testing, leading identity management software tools, and Windows Active Directory.
3. Use the web to find out more about the company, the kinds of systems it uses, and who might be using those systems.

REVIEW SUMMARY

8-1 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. Malware can disable systems and websites, with mobile devices a major target. 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.

8-2 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. 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.

8-3 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 information systems auditing helps organizations determine the effectiveness of security and controls for their information systems.

8-4 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 for suspicious network traffic and attempts to access corporate systems. Passwords, tokens, smart cards, and biometric authentication are used to authenticate system users. Anti-malware software checks computer systems for infections by viruses and worms and often eliminates the malicious software. Encryption, the coding and scrambling of messages, is a widely used technology for securing electronic transmissions over unprotected networks. Blockchain technology enables companies to create and verify tamperproof transactions on a network without a central authority. 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 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), 344
Anti-malware software, 349
Application controls, 342
Authentication, 346
Biometric authentication, 347
Botnet, 333
Bugs, 338
Business continuity planning, 345

Click fraud, 335
Computer crime, 333
Computer forensics, 341
Computer virus, 330
Controls, 327
Cybervandalism, 332
Cyberwarfare, 336
Denial-of-service (DoS) attack, 332

Digital certificates, 351
Digital resiliency, 353
Disaster recovery planning, 345
Distributed denial-of-service (DDoS) attack, 332
Downtime, 353
Drive-by download, 330
Encryption, 350
Evil twin, 334
Fault-tolerant computer systems, 353
Firewall, 348
General controls, 342
Gramm-Leach-Bliley Act, 340
Hacker, 332
HIPAA, 340
Identity management, 346
Identity theft, 334
Information systems audit, 345
Intrusion detection systems, 349
Keyloggers, 332
Malware, 330
Managed security service providers (MSSPs), 353
Online transaction processing, 353
Password, 346
Patches, 339
Pharming, 334
Phishing, 334
Public key encryption, 351
Public key infrastructure (PKI), 351
Ransomware, 331
Risk assessment, 343
Sarbanes-Oxley Act, 340
Secure Hypertext Transfer Protocol (S-HTTP), 350
Secure Sockets Layer (SSL), 350
Security, 327
Security policy, 343
Smart card, 347
Sniffer, 332
Social engineering, 336
Spoofing, 332
Spyware, 332
SQL injection attack, 331
Token, 347
Trojan horse, 331
Two-factor authentication, 347
Unified threat management (UTM), 350
War driving, 329
Worm, 330
Zero-day vulnerabilities, 339

MyLab MIS

To complete the problems with MyLab MIS, go to the EOC Discussion Questions in MyLab MIS.

Review Questions

8-1 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 employees create.
- Explain how software defects affect system reliability and security.

8-2 What is the business value of security and control?

- Explain how inadequate security and control may result in serious legal liability.
- Define the term electronic evidence and explain its importance.

8-3 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 information systems auditing promotes security and control.

8-4 What are the most important tools and technologies for safeguarding information resources?

- Describe the nature of a token in the context of authentication.
- Describe how two-factor authentication can help to reduce fraud, hacking, and security breaches.

- Explain how an intrusion detection system works.
- Explain why an organization might choose to use a unified threat management system.
- Explain how a digital certificate works and why it might give a site visitor a greater sense of security.
- Explain why small businesses in particular might opt to use managed security service providers.
- Explain how employing software metrics can improve system quality and reliability.

Discussion Questions

8-5 MyLab MIS Security isn't simply a technology issue, it's a business issue. Discuss.

8-6 MyLab MIS If you were developing a business continuity plan for your company, where would you start? What aspects of the business would the plan address?

8-7 MyLab MIS Suppose your business had an e-commerce website where it sold goods and accepted credit card payments. Discuss the major security threats to this website 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. Visit MyLab MIS to access this chapter's Hands-On MIS Projects.

Management Decision Problems

8-8 VidHongKong is planning a new Internet venture for renting and watching movies online. Their planned solution comprises a newly built web portal, a new database for keeping records of movies, movie rentals, and customers; a new CRM system; and specialized software for connecting the new system to their existing information system. Perform a security analysis for the new venture. Consider examples of risks for the new website, the new database, the new CRM system, the link to the existing information system, and the end products (the movies).

8-9 A survey of your firm's IT infrastructure has identified a number of security vulnerabilities. Review the data about these vulnerabilities, which can be found in a table in MyLab MIS. Use the table to answer the following questions:

- Calculate the total number of vulnerabilities for each platform. What is the potential impact on the organization of the security problems for each computing platform?
- 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 these vulnerabilities illustrate 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

8-10 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 that management requested identified a number of potential exposures. These exposures, their associated probabilities, and average losses are summarized in a table, which can be found in MyLab MIS. 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

8-11 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 of whether 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.

Collaboration and Teamwork Project

Evaluating Security Software Tools

8-12 With a group of three or four students, use the web to research and evaluate security products from two competing vendors, such as for anti-malware software, firewalls, or antispyware software. For each product, describe its capabilities, for what types of businesses it is best suited, and its cost to purchase and install. Which is the best product? Why? If possible, use Google Docs and Google Drive or Google Sites to brainstorm, organize, and develop a presentation of your findings for the class.