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

- The Electric Power Grid Becomes a Cyberwarfare Battleground
- Meltdown and Spectre Haunt the World's Computers
- Phishing for Money: Dangerous Emails
- 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

THE ELECTRIC POWER GRID BECOMES A CYBERWARFARE BATTLEGROUND

The US electricity grid is a complex digital and physical system critical to commerce and daily life. It consists of more than 7,000 power plants, 55,000 electrical substations, 160,000 miles of high-voltage transmission lines, and 5.5 million miles of low-voltage distribution lines. This web of generators, substations, and power lines is organized into three major interconnections operated by 66 balancing authorities and 5,000 different utilities. The grid has many points of vulnerability, which can be abused by hackers who penetrate computer systems. Incursions into the US electric grid have been going on since at least 2013.

These hacker attacks have the capability to bring down all or part of electricity service throughout the United States. A cyberattack could black out a large region of the nation for weeks or even months, resulting in loss of life support systems in hospitals, disruption of clean water supplies and sanitation, and massive breakdowns of financial and transportation systems. A 2015 Lloyds of London study found that a cyberattack on 50 generators in the Northeast could leave 93 million people without power and cost the economy over $234 billion.

Over the past several years Russian hackers have targeted a Vermont utility, power grids in Ukraine and Ireland, a US nuclear plant, and US energy companies. Russian hacking activity against the United States has been rising as the overall US–Russia relationship hits new lows, evidenced most dramatically by Russian hacker interference in the 2016 presidential election. According to the Department of Homeland Security (DHS) and the FBI, Russia now appears to be laying a foundation for a large-scale cyberattack on US infrastructure. The DHS has identified the electric power grid hackers as a group with Russian government ties known as Dragonfly or Energetic Bear.

The North American Electric Reliability Corporation, which oversees the grid in the United States and Canada, has issued standards and guidelines for how electric companies should protect the power grid physically and electronically. These standards and guidelines have helped power plants and high-voltage transmission networks become more secure, but security still lags at low-voltage distribution networks supplying power directly to homes and workplaces.

© Igor Stevanovic / 123RF

Especially vulnerable are systems used by contractors and subcontractors to service the power grid, which are less prepared for hacker intrusions. Russian hackers were able to access these smaller systems as

a backdoor into the US electric grid. To obtain user names and passwords for accessing grid networks, the hackers planted malicious software on websites catering to utility engineers and sent out emails with tainted attachments. In some cases the hackers were able to penetrate systems that monitor and control electricity flows. Some big utility systems, such as the Bonneville Power Administration and PacifiCorp, were targeted, as well as several energy companies that build systems supplying emergency power to Army bases.

The United States and other countries may be vulnerable, but they have not been sitting still. Since 2012 the United States has put reconnaissance probes inside the control systems of the Russian electric power grid. In June 2019 the United States ramped up its digital power grid incursions to signal the Trump administration's willingness to deploy cybertools more aggressively. The United States inserted potentially crippling malware inside Russia's grid and other targets in addition to more public actions directed at Russia's misinformation and hacking activities during US elections. These new cyberincursions serve partially as a warning but also as preparation for future cyberstrikes if a major US–Russian conflict erupts. They also increase the chances of a major cyberconfrontation.

Sources: Rebecca Smith and Bob Barry, "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It," *Wall Street Journal*, January 10, 2019; David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *New York Times*, June 15, 2019; Shelby Lin Erdman, "How Vulnerable Is the U.S. Power Grid to a Cyberattack? 5 Things to Know," *AJC*, March 19, 2018; Melanie Kenderdine and David Jermain, "U.S. Power Grid Needs Defense against Looming Cyberattacks," *The Hill*, March 23, 2018; and Manimaran Govindarasu and Adam Hahn, "Cybersecurity and the Power Grid: A Growing Challenge," *The Conversation*, February 23, 2017.

Foreign hacker efforts to penetrate and disrupt the US electric power grid illustrate some of the reasons why organizations need to pay special attention to information systems security. The IT security breaches that enabled Russian hackers to break into information systems used in the US power grid have the potential to shut down critical infrastructure throughout the country, paralyzing business, government, and daily life. Weak IT security has been responsible for many billions of dollars of corporate and consumer financial losses in other areas as well.

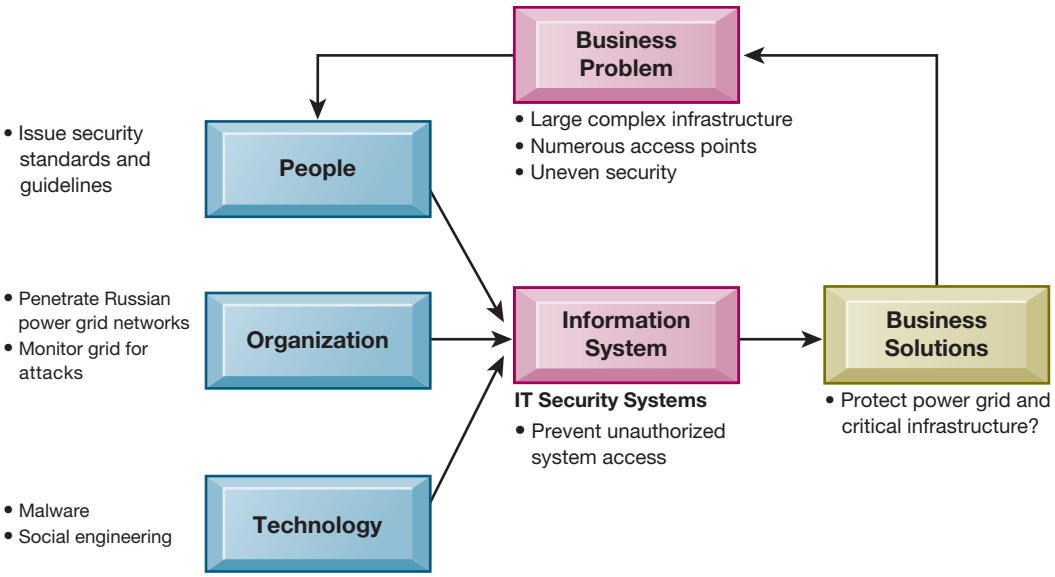
The chapter-opening diagram calls attention to important points raised by this case and this chapter. The US electric power grid is large and complex, with many unguarded points of entry for malicious intruders. Smaller organizations using the power grid lacked the awareness, resources, and tools to prevent employees from naïvely responding to hacker ploys to obtain authentication information for accessing power grid systems.

The United States has taken countermeasures to break into Russian power grid systems, but needs better technology, education, and procedures for unprotected portions of its own grid. What has happened so far is serious and most likely a preview of future incursions into critical systems. Equally disturbing, the security vulnerabilities that facilitated the US power grid hacks are commonplace in businesses and other organizations as well.

Here are some questions to think about: What security vulnerabilities were exploited by the hackers? What people, organizational, and technological factors contributed to these security weaknesses? What was the business impact of these problems? Could the US power grid hacking have been prevented?

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 against contemporary

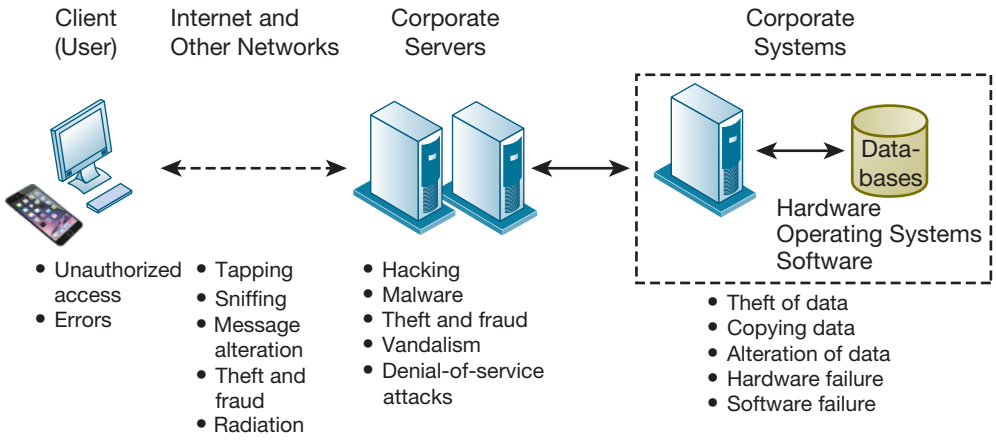


Figure 8.1 Contemporary Security Challenges and Vulnerabilities.
The architecture of a web-based application typically includes a web client, a server, and corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities. Floods, fires, power failures, and other electrical problems can cause disruptions at any point in the network.

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 the Internet and other 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 mobile phones 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. Data stored in some cloud systems can be at risk if the systems are not used or configured properly.

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. Wireless networks in many locations do not have basic protections against **war driving**, in which eavesdroppers drive by buildings or park outside and try to intercept wireless network traffic.

Intruders can use the information they have gleaned from a Wi-Fi network to set up rogue access points on a different radio channel in a nearby physical location to force a Wi-Fi user 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.) It is estimated that 350,000 new malware variants are discovered every day (Akamai, 2019). 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; from compromised email messages, online ads, or instant messaging; and from public cloud data storage services. Especially prevalent today are **drive-by downloads**, consisting of malware that comes with a downloaded file that a user intentionally or unintentionally requests.

Hackers can do to a smartphone just about anything they can do to any Internet-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

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 more than 5 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.

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, a malware strain called FacexWorm appeared inside Facebook Messenger in 2018. Clicking a link via Facebook Messenger takes the victim to a fake YouTube page, which tries to trick the user into installing a YouTube extension for the popular Chrome browser. From there the malware can steal passwords or try to steal cryptocurrency funds such as Bitcoin.

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. Additional 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, the ransomware called WannaCry that attacked computers in more than 150 countries in May 2017 encrypts an infected computer's files, forcing users to pay hundreds of dollars to regain access. In 2019, twenty-two Texas cities were held hostage for millions of dollars after a hacker or hacker group infiltrated their computer systems and encrypted their data (Fernandez, Sanger, and Martinez, 2019). 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. 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 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 numerous 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 zombie PCs infected with malicious software without their owners' knowledge and organized into a **botnet**. Hackers create these botnets by infecting other people's computers with bot malware that opens a back door through which an attacker can give instructions. The infected computer then becomes a slave, or zombie, serving a master computer belonging to someone else. 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. An 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.

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.

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

Computer crime is defined by the US 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 the Ponemon Institute's 2018 Annual Cost of Cyber Crime Study, the average annualized cost of cybercrime security for benchmarked companies in 11 different countries and 16 industries was $13 million (Ponemon Institute, 2019). Many companies are reluctant to report computer crimes because the crimes may involve employees or the companies fear 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 (see the chapter-ending case study). According to the 2019 Identity Fraud Study by Javelin Strategy & Research, identity fraud affected 14.4 million consumers in 2018 (Javelin, 2019).

One increasingly 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 asking users for confidential personal data, such as Social Security numbers or bank and credit card information, 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 that 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's 2018 Cost of a Data Breach Study, the average global cost of a data breach among the companies it surveyed was $3.86 million (Ponemon, 2018). 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 US 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.

TABLE 8.3

Major Data Breaches

Country	Description of Data Breach
United Kingdom	British Airways experienced a data breach in 2018 in which hackers stole the personal and financial details of customers who made, or changed, bookings on ba.com or its app during that time. Names, email addresses and credit card information were stolen, including card numbers, expiration dates and the three digit CVC code required to authorize payments. Around 380,000 transactions were affected..
United Arab Emirates	In 2018 cybercriminals stole data from 14 million customer records from ride-hailing firm Careem and an unnamed airline customer, including names, email addresses, phone numbers and trip details in the Middle East, North Africa and South Asia..
Sweden	In 2018, the government announced a huge data breach of personal records from the Swedish Transport Agency's project with IBM to update Sweden's vehicle registration system. The breach was not caused by hackers but by failure to install security safeguards by IBM. The breach was not announced for18 months after it occurred.
Singapore	In 2018, SingHealth, the country's largest group of healthcase institutions, reported a data breach, compromising personal data of 1.5 million healthcare patients, including that of its Prime Minister Lee Hsien Loong. The stolen data for each patient included name, national identification number, address, gender, race, and date of birth.
Malaysia	The Malaysian government revealed the largest data breach in Asia in 2017 involving 46 million mobile phone accounts, larger than the entire Malaysian population. The data leaked included mobile phone numbers, ID card numbers, home addresses and SIM card data from at least 12 mobile phone and network operators in Malaysia..

US 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 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. A proposed federal Data Security and Breach Notification Act would mandate organizations that possess personal information to put in place "reasonable" security procedures to keep the data secure and notify anyone affected by a data breach, but it has not been enacted.

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. 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 the efforts of Russian hackers to disrupt the US 2016 presidential elections and to penetrate the US power grid, described in the chapter-opening case. 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 even 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 for the oil and water pipelines and power grid of the United States and have 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 US 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. US 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. For example, in July 2019 a former employee at Amazon Web Services used her knowledge of Amazon cloud security to steal 106 million Capital One Financial records stored by Amazon's cloud computing service (McMilan, 2019a).

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-messaging application that allowed attackers to install spyware on mobile phones (McMillan, 2019b).

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. For example, in December 2018 Microsoft had to release an emergency update for a zero-day vulnerability in its Internet Explorer web browser software that gives an outside intruder access to a computer's memory. The memory corruption could have enabled an attacker to have the same access to a computer system as a valid logged-in user (Kerner, 2018). 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 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

The Interactive Session on Technology describes newly discovered vulnerabilities stemming 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.

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

Companies have valuable information assets to protect. Systems often house confidential information about individuals' taxes, financial assets, medical records, and job performance reviews. They also can contain information on corporate operations, including trade secrets, new product development plans, and marketing strategies. Government systems may store information on weapons systems, intelligence operations, and military targets. These information assets have tremendous value, and the repercussions can be devastating if they are lost, destroyed, or placed in the wrong hands. Systems that are unable to function because of security breaches, disasters, or malfunctioning technology can 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, Target had to pay $39 million to several US 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 for the retention and storage of electronic records as well as for privacy protection.

Meltdown and Spectre Haunt the World's Computers

In early January 2018, computer users all over the world were shocked to learn that nearly every computer chip manufactured in the last 20 years contained fundamental security flaws that make it possible for attackers to obtain access to data that were thought to be completely protected. Security researchers had discovered the flaws in late 2017. The flaws arise from features built into the chips that help them run faster. The vulnerability enables a malicious program to gain access to data it should never be able to see.

There are two specific variations of these flaws, called Meltdown and Spectre. Meltdown was so named because it "melts" security boundaries normally enforced by hardware. By exploiting Meltdown, an attacker can use a program running on a computer to gain access to data from all over that machine that the program shouldn't normally be able to see, including data belonging to other programs and data to which only administrators should have access. (A system administrator is responsible for the upkeep, configuration, and reliable operation of computer systems.) Meltdown affects only specific kinds of Intel chips produced since 1995.

Spectre is not manufacturer-specific and affects nearly all modern processors. It requires more intimate knowledge of the victim program's inner workings. Spectre's name comes from speculative execution, in which a chip is able to start work on predicted future operations in order to work faster. In this case, the system is tricked into incorrectly anticipating application behavior. The name also suggests that Spectre will be much more difficult to neutralize. Other attacks in the same family will no doubt be discovered, and Spectre will be haunting us for some time.

With both Meltdown and Spectre, an attacker can make a program reveal some of its own data that should have been kept secret. For example, Spectre could harness JavaScript code on a website to trick a web browser into revealing user and password information. Meltdown could be exploited to view data owned by other users and also virtual servers hosted on the same hardware, which is especially dangerous for cloud computing host computers. The most worrisome aspect of Meltdown and Spectre is that security vulnerabilities are not from flawed software but from the fundamental design of hardware platforms beneath the software.

There is no evidence that Spectre and Meltdown have been exploited, but this would be difficult to detect. Moreover, the security flaws are so fundamental and widespread that they could become catastrophic, especially for cloud computing services where many users share machines. According to researchers at global security software firm McAfee, these vulnerabilities are especially attractive to malicious actors because the attack surface is so unprecedented and the impacts of leaking highly sensitive data are so harmful. According to Forester, performance of laptops, desktops, tablets, and smartphones will be less affected. The fundamental vulnerability behind Meltdown and Spectre is at the hardware level, and thus cannot be patched directly.

Major technology vendors are only able to release software fixes that work around the problems. Such fixes mitigate vulnerabilities by altering or disabling the way software code makes use of speculative execution and caching features built into the underlying hardware. (Caching is a technique to speed computer memory access by locating a small amount of memory storage on the CPU chip rather than from a separate RAM chip for memory.) Since these features were designed to improve system performance, working around them can slow systems down. Experts initially predicted system performance could be degraded as much as 30 percent, but a slowdown of 5 to 10 percent seems more typical.

Cloud vendors have taken measures to patch their underlying infrastructures, with their customers expected to install the patches for their operating systems and applications. Microsoft released operating system patches for Windows 7 and all later versions, which also apply to Microsoft's Internet Explorer and Edge browsers. Apple released patched versions of its Safari browser and iOS, macOS, and tvOS operating systems. Google provided a list of which Chromebook models will or won't need patches and released a patch for its Chrome browser. Older operating systems such as Windows XP and millions of third-party low-cost Android phones that don't get security updates from Google will most likely never be patched. Organizations should apply updates and patches to browser software as soon as they are available. And since these vulnerabilities could enable attackers to steal passwords from user device memory when running JavaScript from a web page, it

is recommended that users be instructed to always close their web browsers when not in use. Forrester also recommends that enterprises should use other techniques to protect data from users and organizations that have not applied the fixes.

Chip manufacturer Intel has issued a number of work-around updates for its processors. These microcode patches have been installed on every Intel CPU sold since the new code's release, but there are still hundreds of millions of systems in the field that might need the update. The only way to truly fix Meltdown and Spectre is to replace affected processors. Redesigning and producing new processors and architectures may take five to ten years to hit the market. If anything good can be said about Spectre and Meltdown, it is that they have focused more global attention on software and hardware security and the need to develop more robust system architectures for secure computing.

Sources: Curtis Franklin Jr., "How Intel Has Responded to Spectre and Meltdown," *Information Week*, January 4, 2019; James Senders, "Spectre and Meltdown Explained: A Comprehensive Guide for Professionals." *TechRepublic*, May 15, 2019; Josh Fruhlinger, "Spectre and Meltdown Explained: What They Are, How They Work, What's at Risk," *CSO*, January 15, 2018; and Warwick Ashford, "Meltdown and Spectre a Big Deal for Enterprises," *Computer Weekly*, January 9, 2018.

CASE STUDY QUESTIONS

1. How dangerous are Spectre and Meltdown? Explain your answer.
2. Compare the threats of Spectre and Meltdown to cloud computing centers, corporate data centers, and individual computer and smartphone users.
3. How would you protect against Spectre and Meltdown if you were running a public cloud computing center, if you ran a corporate data center, and if you were an individual computer user?

If you work in the U.S. healthcare industry, your firm will need to comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. **HIPAA** outlines medical security and privacy rules and procedures for simplifying the administration of healthcare billing and automating the transfer of healthcare data between healthcare providers, payers, and plans. It requires members of the healthcare industry to retain patient information for six years and ensure the confidentiality of those records. It specifies privacy, security, and electronic transaction standards for healthcare providers handling patient information, providing penalties for breaches of medical privacy, disclosure of patient records by email, or unauthorized network access. In the European Union new regulations impose similar requirements on health care providers (Regulation 679).

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

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

Sarbanes–Oxley is fundamentally about ensuring that internal controls are in place to govern the creation and documentation of information in financial statements. Because information systems are used to generate, store, and transport such data, the legislation requires firms to consider information systems security and

other controls required to ensure the integrity, confidentiality, and accuracy of their data. Each system application that deals with critical financial reporting data requires controls to make sure the data are accurate. Controls to secure the corporate network, prevent unauthorized access to systems and data, and ensure data integrity and availability in the event of disaster or other disruption of service are essential as well.

ELECTRONIC EVIDENCE AND COMPUTER FORENSICS

Security, control, and electronic records management have become essential for responding to legal actions. Much of the evidence today for stock fraud, embezzlement, theft of company trade secrets, computer crime, and many civil cases is in digital form. In addition to information from printed or typewritten pages, legal cases today increasingly rely on evidence represented as digital data stored on portable storage devices, CDs, and computer hard disk drives as well as in email, instant 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.

RISK ASSESSMENT

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

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

Table 8.5 illustrates sample results of a risk assessment for an online order processing system that processes 30,000 orders per day. The likelihood of each exposure occurring over a one-year period is expressed as a percentage. The next column shows the highest and lowest possible loss that could be expected each time the exposure occurred and an average loss calculated by adding the highest and lowest figures 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

TABLE 8.5

Online Order Processing Risk Assessment

Exposure	Probability of Occurrence (%)	Loss Range/Average ($)	Expected Annual Loss ($)
Power failure	30 percent	$5,000–$200,000 ($102,500)	$30,750
Embezzlement	5 percent	$1,000–$50,000 ($25,500)	$1,275
User error	98 percent	$200–$40,000 ($20,100)	$19,698

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 8.2 shows 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 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

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

Figure 8.2
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.

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. For example, Healthways, a well-being improvement company headquartered in Franklin, Tennessee, implemented a business continuity plan that identified the business processes of nearly 70 departments across the enterprise and the impact of system downtime on those processes. Healthways pinpointed its most critical processes and worked with each department to devise an action plan.

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 8.3 is a sample auditor's listing of control weaknesses for a loan system. It includes a section for notifying management of such weaknesses and for management's response. Management is expected to devise a plan for countering significant weaknesses in controls.

8-4 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

Figure 8.3
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		

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. 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 a multistep process. To

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

be authenticated, a user must provide two means of identification, one of which is typically 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 8.4).

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 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.

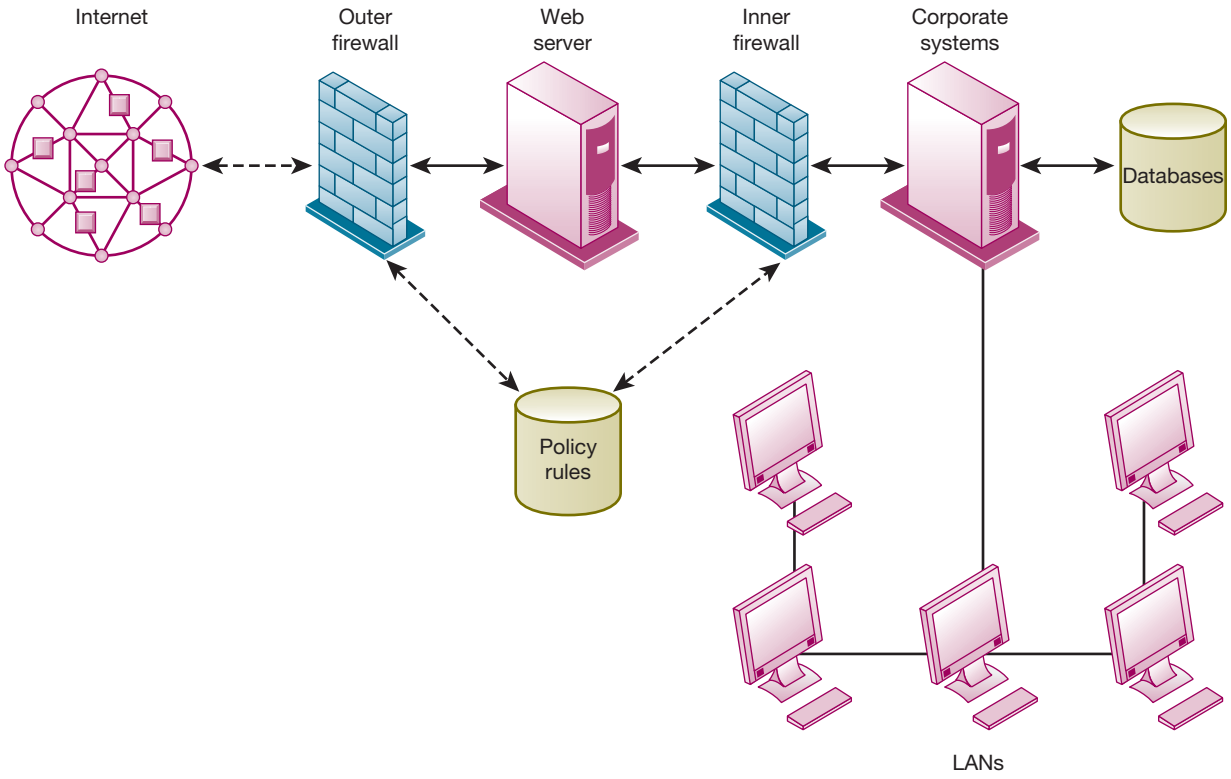


Figure 8.4
A Corporate Firewall.
The firewall is placed between the firm's private network and the public Internet or another distrusted network to protect against unauthorized traffic.

Packet filtering examines selected fields in the headers of data packets flowing back and forth between the trusted network and the Internet, examining individual packets in isolation. This filtering technology can miss many types of attacks.

Stateful inspection provides additional security by determining whether packets are part of an ongoing dialogue between a sender and a receiver. It sets up state tables to track information over multiple packets. Packets are accepted or rejected based on whether they are part of an approved conversation or 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 or cloud service 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. Leading UTM vendors include Fortinent, Sophos, and Check Point, and networking vendors such as Cisco Systems and Juniper Networks provide UTM capabilities in their products.

SECURING WIRELESS NETWORKS

The initial security standard developed for Wi-Fi, called Wired Equivalent Privacy (WEP), was not very effective because its encryption keys were relatively easy to crack. 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 replaced WEP with stronger security standards. The most recent version is WPA3, introduced in 2018. The new standard makes passwords even harder to crack and strengthens user privacy in public networks through individualised data encryption. Corporations can further improve Wi-Fi security by using it in conjunction with virtual private network (VPN) technology when accessing internal corporate data.

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 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 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 8.5. 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 8.6). 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.

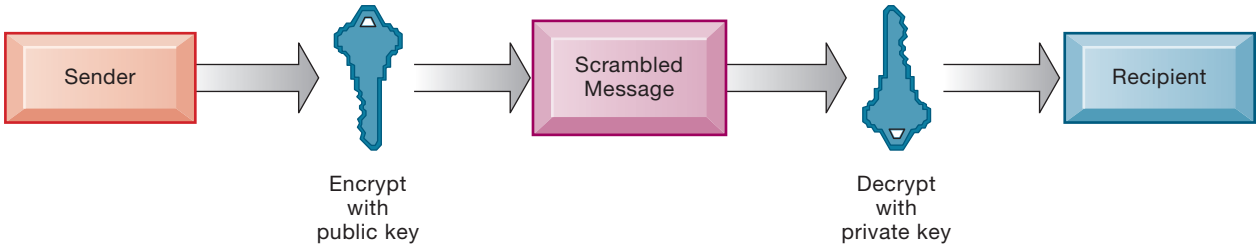


Figure 8.5
Public Key Encryption.
A public key encryption system can be viewed as a series of public and private keys that lock data when they are transmitted and unlock data when they are received. The sender locates the recipient's public key in a directory and uses it to encrypt a message. The message 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.

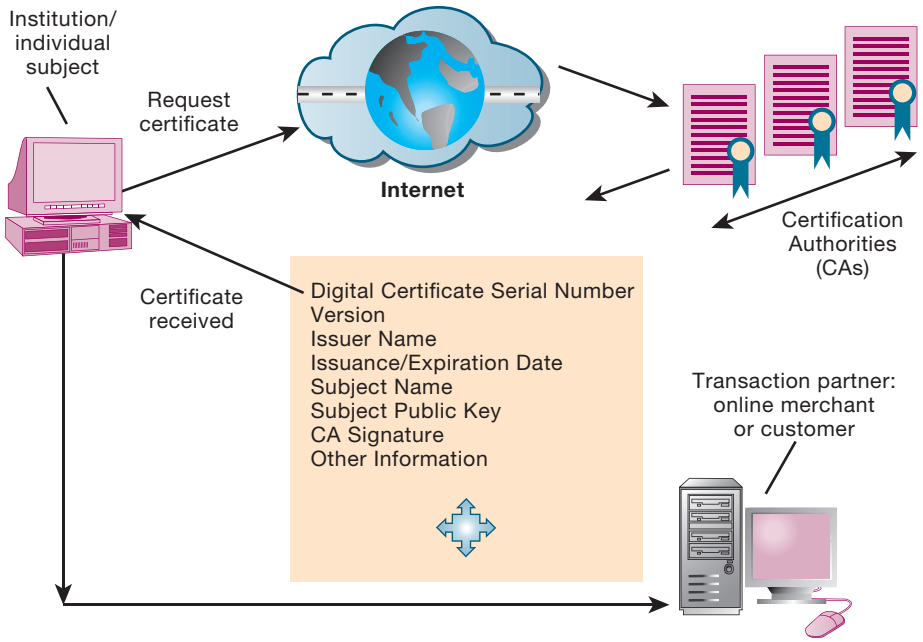


Figure 8.6
Digital Certificates.
Digital certificates help establish the identity of people or electronic assets. They protect online transactions by providing secure, encrypted, online communication.

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. Blockchain is especially suitable for environments with high security requirements and mutually unknown actors.

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 to deliver uninterrupted service, despite one or more components failing. Fault-tolerant computers are able to detect hardware or software failures and automatically switch to a backup capability. Components can be 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, manage firewalls, and perform vulnerability testing and and antiviral and intrusion detection. SecureWorks, AT&T, Verizon, IBM, and Symantec are leading providers of MSSP services.

SECURITY ISSUES FOR CLOUD COMPUTING AND THE MOBILE DIGITAL PLATFORM

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

Security in the Cloud

When processing takes place in the cloud, accountability and responsibility for protection of sensitive data still reside with the company owning that data. Understanding how the cloud computing provider organizes its services and manages the data is critical.

Cloud computing is highly distributed. Cloud applications reside in large remote data centers and server farms that supply business services and data management for multiple corporate clients. To save money and keep costs low, cloud computing providers often distribute work to data centers around the globe where work can be accomplished most efficiently. When you use the cloud, you may not know precisely where your data are being hosted.

Virtually all cloud providers use encryption to secure the data they handle while the data are being transmitted. However, if the data are stored on devices that also store other companies' data, it's important to ensure that these stored data are encrypted as well. DDoS attacks are especially harmful because they render cloud services unavailable to legitimate customers.

Companies expect their systems to be running 24/7. Cloud providers still experience occasional outages, but their reliability has increased to the point where a number of large companies are using cloud services for part of their IT infrastructures. Most keep their critical systems in-house or in private clouds.

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 out 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

Phishing for Money: Dangerous Emails

In 2018, the Dutch branch of Pathé received an email from the cinema conglomerate's headquarters in France. A manager at the French office told the Dutch director and her chief financial officer that there were plans to buy a company in Dubai. Would they transfer the necessary funds? The email certainly looked legitimate. The two Dutch managers made the payment. And again, and again. All in all, they sent $21.7 million. Sadly, the money only ended up in the pockets of digital con artists.

This is an example of "phishing," whereby criminals angle for personal information that they can use for their scams. There are several ways to classify phishing, but a distinction is often made between spear phishing and bulk phishing. The former relates to a phishing attack that is specifically directed at one or two persons—in our example, the director and chief financial officer of Pathé. It would be easy to dismiss these two officials as just exceedingly careless, but in reality, the situation is often more complicated. Many of those who perpetrate phishing attacks do their homework before sending their emails. They often hack the website of the company concerned and study the activity and emails in its system to find out how to make an email more credible. The really dedicated ones even study the writing style of the CEO.

Instances of CEO fraud are usually not publicly revealed, but they can potentially be very successful, according to Ken Bagnall, the head of FireEye, a company that focuses on securing emails. He points to the "CEO fraud test" that was sent to a number of companies. The result was stunning: 90 percent of the companies contacted took the bait. Given this success rate, it may seem surprising that few successful attacks are reported in the news, but it is likely that many go unreported. Data hacks have very negative effects on the reputation of companies; clients trust them less and may take their business elsewhere. Companies are more likely to cut their losses rather than report the fraud to the police. If a phishing attack is successful, the long-term damage to a company likely to be huge.

In the other type of phishing—bulk phishing—emails are sent to thousands, sometimes even millions of people. Many of these emails are easily recognizable as fraudulent; they often, for instance, contain basic language errors. Sometimes, however, even bulk emails look surprisingly professional.

In 2019, Retruster, a company offering anti-phishing software and services, compiled some disturbing statistical data regarding phishing and its incidence. In 2018, phishing attacks increased by 65 percent. According to the company, 30 percent of phishing messages are opened by the recipients and 15 percent of people successfully phished are targeted again within a year. In addition, almost 1.5 million new malicious sites related to phishing are being created every month.

The big problem is that phishing has become much more professional as well as cheaper. Most links in the phishing emails are to malicious websites that may replicate the website of an actual bank. For instance, Dutch state broadcaster NOS discovered in 2018 that a Russian site called Boris was selling fake copies of a Dutch bank's website for only $296.

What can companies and individuals do to protect themselves against phishing attacks? The first answer to that question is very simple: be cautious. Even today, phishing emails contain telltale mistakes in grammar. A threat or warning is also a sign that something is amiss; in such instances, banks advise customers to call in just to check if the email was really sent by the bank.

The second answer is to use security software and update it regularly. Antivirus software programs typically include a list of suspicious websites. Once the recipient of a phishing email is directed toward a malicious site, the antivirus will block it.

Some security experts suggest a third and more extreme answer: make sure that emails never have attachments. Phishing emails often rely on them to make sure that the scam is successful, so in theory this is a good precaution; unfortunately, in practice, it is virtually impossible to send out emails without attachments.

However, even if all possible measures are taken, phishing emails may yet be successful, and it only takes one to cause real trouble for the company. Ken Bagnall, the CEO of The Email Laundry, highlights the dangerous situation that is created once the email account of a CEO is hacked: cybercriminals could then send out emails with every appearance of being the real thing, potentially doing enormous damage.

Sources: "Phishing and Email Fraud Statistics 2019," retruster.com, accessed January 2020; "Pathé Verliest 19 Miljoen Door Ceo-Fraude," Avrotros, November 12, 2018, opgelicht.avrotros.nl, accessed January 12, 2019; "'Boris' Verkoopt Nagemaakte Nederlandse Banksites Voor 262 Euro," NOS, November 25, 2018, nos.nl, accessed January 12, 2019; Eitan Katz, "Phishing Statistics: What Every Business Needs to Know," Dashlane, January 17, 2018, blog.dashlane.com; Joost Schellevis, "OUCH! Newsletter: CEO Fraud," SANS Security Awareness, July 2016, www.sans.org; Eleanor Dallaway, "#ISC2CongressEMEA: Why CEO Fraud Works and How to Stop It," *Infosecurity Magazine*, October 19, 2016, www.infosecurity-magazine.com.

CASE STUDY QUESTIONS

1. Explain the difference between spear phishing and bulk phishing. Which of the two forms of phishing do you think is most difficult to spot by victims, and why?
2. The CEO of your company received a fraudulent email and made a payment to digital criminals. He wonders now whether he should contact the police. What factors should he take into consideration before taking a decision?
3. Dashlane advises clients to send emails without attachments. Do you think that not adding attachments to emails will help protect companies against phishing stacks?
4. Give two pieces of advice to a company or individual on increasing protection against a phishing attack.

Case contributed by Bernard Bouwman

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 stored, 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 12. 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 is a major supermarket grocery store chain located in the UK. They are looking to fill an entry-level position for an identity access and management support specialist. The company over 500 stores, more than 8,000 workers, and nearly a million weekly 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), 312
Anti-malware software, 317
Application controls, 310
Authentication, 314
Biometric authentication, 314
Botnet, 301
Bugs, 305
Business continuity planning, 313
Click fraud, 304
Computer crime, 301
Computer forensics, 309
Computer virus, 299
Controls, 297
Cybervandalism, 301
Cyberwarfare, 304
Denial-of-service (DoS) attack, 301
Digital certificates, 318
Disaster recovery planning, 312
Distributed denial-of-service (DDoS) attack, 301
Downtime, 319
Drive-by download, 299
Encryption, 317
Evil twin, 303
Fault-tolerant computer systems, 319
Firewall, 315
General controls, 310
Gramm–Leach–Bliley Act, 308
Hacker, 301
HIPAA, 308
Identity management, 313
Identity theft, 302
Information systems audit, 313
Intrusion detection systems, 316
Keyloggers, 300
Malware, 299
Managed security service providers (MSSPs), 320
Online transaction processing, 319
Password, 314
Patches, 306
Pharming, 303
Phishing, 302
Public key encryption, 318
Public key infrastructure (PKI), 318
Ransomware, 300
Risk assessment, 311
Sarbanes–Oxley Act, 308
Secure Hypertext Transfer Protocol (S-HTTP), 317
Secure Sockets Layer (SSL), 317
Security, 297
Security policy, 311
Smart card, 314
Sniffer, 301
Social engineering, 305
Spoofing, 301
Spyware, 300
SQL injection attack, 300
Token, 314
Trojan horse, 300
Two-factor authentication, 314
Unified threat management (UTM), 317
War driving, 298
Worm, 299
Zero-day vulnerabilities, 305

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?
- Distinguish between implementation and administrative controls.
- What are general controls, and what do they apply to in information systems?
- Describe how systems builders decide which controls are necessary.
- 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 identification 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.

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

Discussion Questions

8-5 MyLab MIS **Information system** 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.

BUSINESS PROBLEM-SOLVING CASE

BULGARIA: A WHOLE NATION HACKED

In July 2019, an anonymous hacker emailed Bulgarian media outlets to proclaim that they had gained access to the database of the Bulgarian tax service. As is often the case with hacks, many of the details are still unclear, but one thing stood out: this was an attack of a staggering scope. Bulgaria has a population of around 7 million people, and the Bulgarian news media reported that the hacker had gained access to the data of 5 million. Analysts quickly concluded that almost everyone who pays taxes in the country had been hacked. The precise data that were accessed is not entirely clear, but it is certain that vital information like names, addresses, data regarding income, and social security numbers had been compromised.

The incident prompted a flurry of questions in the press and online: Who did it? How did it take place—what vulnerabilities in the tax service's systems did the hacker use to gain access? Could it have been prevented? Were the Bulgarian authorities sloppy, or were their cybersecurity efforts the best that could be expected and the hack unavoidable? Most importantly, what was the impact of this hack, both for the 5 million Bulgarians whose data had been accessed and the Bulgarian authorities?

The first question has yet to be adequately answered. The Bulgarian police, undoubtedly under severe pressure to produce a suspect, briefly detained Kristiyan Boykov, a young "computer wizard" employed by a firm focusing on cybersecurity. It was believed that he had perpetrated the attack to make the point that Bulgaria needed to do more to protect its data. In 2017, he had exposed vulnerabilities in the website of the Bulgarian Ministry of Education, and he subsequently gave an interview on Bulgarian television explaining that he had exposed these flaws as a matter of "civic duty."

The then 20-year-old suspect denied all involvement and was released, though prosecutors continue to insist that he is the main culprit, conceding only that others may have been involved as well. They point to an email linked to the hack that was sent from one of the computers in Boykov's possession. When the hack took place, it was assumed to be an attack from outside the country, for the email in which the hack was announced had been sent from a Russian IP address. However, as the investigation progressed, it became clear that this IP address was simply a smokescreen and the email had in fact originated within Bulgaria.

What vulnerabilities did the hacker exploit? A final answer can only be given once a thorough investigation of the hack is concluded, but cybersecurity experts in Bulgaria quickly concluded that the attack was perpetrated through a system created to file VAT returns from outside Bulgaria. They identified it as an SQL injection, which takes place when corrupted input is fed into a system; instead of performing the tasks that it is supposed to, the system performs the orders it received through the corrupted input. SQL injections are often explained using the metaphor of a fully automated bus: it obeys the commands it gets and will halt at the right stops if it is told to, but if the commands are corrupted, the bus may, for instance, halt every three minutes whether there is a stop or not.

Could the hack have been prevented? Looking at the statistics, it becomes clear that the Bulgarian hack is not the not the only one to have been perpetrated by using an SQL injection; in 2017, as many as 20 percent of all cyberattacks were carried out by the same method. However, there are ways to protect computer systems against such an attack, and they are not complicated. One of these, is, of course, to use the right software and make sure that the patches for it are applied as soon as they become available. A powerful protection against SQL injection in particular is the use of so-called prepared statements. By using such statements, only certain input is accepted: to use the metaphor of the bus again, you cannot simply, for instance, tell the bus to stop all the time; you can only enter the name of specific streets.

As always, suspicion is a powerful protective tool in cybersecurity. When dealing with sensitive data, it is important to monitor access to the system that hosts it and, importantly, log and study unsuccessful efforts to send input (which sometimes prove to be an attempt to hack the system). It is also useful to try hacking your own system; if the Bulgarian tax service had enlisted its own "hacking squad," they would surely have found the vulnerability early on and prevented the attack.

None of these strategies were in place in Bulgaria, according to the country's cybersecurity experts. The hacker boasted of having obtained access to the system several years before the date of the actual attack, and the email announcement to the press

contemptuously referred to cybersecurity in Bulgaria as a "parody" of a real one. That may be a harsh judgment, but it is true that many experts had issued the same warnings as the hacker for a long time. Indeed, several months before the tax database hack, the Commercial Registry of Bulgaria was attacked as well. After the tax hack took place, it became clear that the Commercial Registry had yet another vulnerability: anyone could gain access to thousands of social security numbers stored on the website of the Commercial Registry merely by performing a search on Google.

The scale and depth of the tax hack, however, alerts us to the fact that official databases and systems around the world have been frequently attacked. One of the most spectacular hacks of a government agency took place in February 2016, causing the Central Bank of Bangladesh to lose more than $100 million. The loss of money would have been much higher—the hackers targeted a total of around a billion dollars—but for mistakes in the wiring instructions that caused several orders to transfer money from the bank to be blocked in the United States. Investigations into the causes and perpetrators of this this hack are still ongoing.

In January 2019, Germany was shocked by one of the biggest data hacks in recent history when very personal details of major politicians (including Chancellor Angela Merkel) were published on Twitter. The German authorities immediately stressed that no really sensitive information had been accessed, but the hack was a huge embarrassment nonetheless, compounded by the fact that the data had been online for several months before their discovery. To add insult to injury, the hack had been perpetrated by a 20-year-old student using commonplace techniques.

The Bulgarian case, however, stands apart as the hack had targeted data from almost everyone in the country who pays taxes. But what made cybersecurity in Bulgaria particularly vulnerable—allegedly the real motivation behind the 2019 hack? To begin with, Bulgarian authorities make a distinction between critical infrastructure and non-critical databases. Critical infrastructure is mostly linked to defense facilities and systems. Bulgaria is a member of NATO, so non-members could try to gain access to Bulgarian defense systems to spy on the alliance, hence their categorization as critical. The tax databases were not considered critical and thus received less attention from the state's cybersecurity experts.

These experts are urging the Bulgarian authorities to step up their efforts to protect their data systems because the impact of such hacks is potentially devastating. Hackers often sell data to criminal gangs, and the data of tax-paying Bulgarians are especially interesting to them as they do not change quickly: people do not change houses or addresses every year and, generally speaking, their income does not fluctuate dramatically either. After the 2019 tax hack, *The New York Times* cited one cybersecurity expert as saying that the data obtained could easily be sold for about $200 million. The Bulgarian news media have already reported fraudulent schemes mostly targeting the elderly in the country, though it is not clear if there is a clear link with the tax hack.

Sadly, the risks will remain in place for many years to come, with two in particular standing out: credit card fraud and identity theft. According to some reports in the Bulgarian news media, the hacked income data goes as far back as 2007. It would be easy for criminals to use this data to make lists of people in Bulgaria who are more affluent and use credit cards. Fortunately, credit card use is not widespread in Bulgaria, but if criminals do succeed in perpetrating this kind of fraud, the costs for both the individual and the bank in question may be huge. There is a huge political price for the Bulgarian authorities to pay as well. Tax-paying citizens need to be sure that their data are being kept safe. Few people like paying taxes to begin with, but they should never feel that they put their financial security at risk the next time they file a tax report.

Bulgaria is a member of the European Union and must abide by the General Data Protection Regulation, a strict set of rules that obliges governments and companies to protect the privacy of citizens and clients. The tax authority was fined €3 million for the breach of data by the country's privacy watchdog. While many of the Bulgarians whose data were illegally accessed may feel that this fine is justified, experts say that this does not solve the problem: Bulgaria needs to take steps to hire more cybersecurity experts and review the security of all data systems.

However, being a member of the European Union has added another wrinkle to Bulgaria's cybersecurity problems. Cybersecurity experts are in short supply thanks to freedom of movement, as talented IT workers can easily migrate from Bulgaria to other member states of the European Union where the salaries are more competitive than what the Bulgarian government offers. This point was forcefully made by Boyko Borissov, the Prime Minister of Bulgaria, after the attack on the tax database took place. According to him, the Bulgarian state pays cybersecurity experts a monthly salary of around 1,500 Bulgarian leva (approximately €770), but in the private sector the starting salary is at least six times that amount.

Prime Minister Borissov also said that he had considered the idea of outsourcing Bulgarian cybersecurity to experts in other countries, but the costs had proven prohibitive. Aside from the troubling legal implications of giving foreigners access to the sensitive data of Bulgarian citizens, the government would have to trust that the systems of the company it had hired were safe themselves—sadly, that is not always the case. The Bulgarian government is now working on a project to create a special cybersecurity unit consisting of experts who are paid well above the average Bulgarian salary.

Sources: Bill Bostock, "A Hacker Broke into Bulgaria's Tax System and Stole the Details of Every Working Adult in the Country," *Business Insider*, July 22, 2019; Alexander Kolev, "Cybersecurity Is Tragic Despite Millions Spent," Sega, July 19, 2019, www.segabg.com; Marc Santora, "5 Million Bulgarians Have Their Personal Data Stolen in Hack," *The New York Times*, July 17, 2019, www.nytimes.com; Tsvetelia Tsolova and Angel Krasimov, "'Wizard' Cybersecurity Expert Charged with Record Hack of Bulgarian Tax Agency," Reuters, July 16, 2019; Kate Connolly, "German Cyber Attack: Man Admits Massive Data Breach, Say Police," *The Guardian*, January 8, 2019, www.theguardian.com; "Hacked: The Bangladesh Bank Heist," Al-Jazeera, May 24, 2018, www.aljazeera.com; Information Security Office, "How to Protect Against SQL Injection Attacks," University of California Berkeley, security.berkeley.edu.

CASE STUDY QUESTIONS

8-13 Identify and describe the security and control issues related to the hacking technique discussed in this case.

8-14 What managerial issues are faced by Bulgarian civil servants in charge of cybersecurity?

8-15 Discuss the potential impact of the Bulgarian tax hack.

8-16 How can data breaches like this be prevented?

Case contributed by Bernard Bouwman, Avans University of Applied Sciences

Chapter 8 References

Akamai Technologies. "What Is Malware?" www.akamai.com, accessed June 27, 2019.

Anderson, Chad, Richard L. Baskerville, and Mala Kaul. "Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information." *Journal of Management Information Systems* 34, No. 4 (2017).

Bauer, Harald, Ondrej Burkacky, and Christian Knochenhauer. "Security in the Internet of Things." *McKinsey and Company* (May 2017).

Bose, Idranil, and Alvin Chung Man Leung. "Adoption of Identity Theft Countermeasures and Its Short- and Long-Term Impact on Firm Value." *MIS Quarterly* 43, No. 1 (March 2019).

Carson, Brant, Giulio Romanelli, Patricia Walsh, and Askhat Zhumaev. "Blockchain Beyond the Hype: What Is the Strategic Business Value?" *McKinsey and Company* (June 2018).

Cloud Standards Customer Council. "Security for Cloud Computing: Ten Steps to Ensure Success, Version 3.0" (December 2017).

Cram, W. Alec, John D'Arcy, and Jeffrey G. Proudfoot. "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance." *MIS Quarterly* 43, No. 2 (June 2019).

Esteves, Jose, Elisabete Ramalho, and Guillermo de Haro. "To Improve Cybersecurity, Think Like a Hacker." *MIT Sloan Management Review* (Spring 2017).

Federal Bureau of Investigation. "2018 Internet Crime Report" (2018).

Fernandez, Manny, David E. Sanger, and Marina Trahan Martinez. "Ransomware Testing Resolve of Cities Across America." *New York Times* (August 22, 2019).

Goode, Sigi, Hartmut Hoehle, Viswanath Venkatesh, and Susan A. Brown. "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach." *MIS Quarterly* 41, No. 3 (September 2017).

Gwebu, Kholekile L., Jing Wang, and Li Wang. "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management." *Journal of Management Information Systems* 35, No. 2 (2018).

Hui, Kai-Lung, Seung Hyun Kim, and Qiu-Hong Wang. "Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks." *MIS Quarterly* 41, No. 2 (June 2017).

Iansiti, Marco, and Karim R. Lakhani. "The Truth About Blockchain." *Harvard Business Review* (January–February 2017).

Javelin Strategy & Research. "2019 Identity Fraud Study" (March 6, 2019).

Kaminski, Piotr, Chris Rezek, Wolf Richter, and Marc Sorel. "Protecting Your Digital Assets." *McKinsey & Company* (January 2017).

Kaspersky Lab. "Kaspersky Finds Mobile Malware Attacks Doubling from 2018." *TechBarrista* (March 12, 2019).

Kerner, Sean Michael. "Microsoft Patches Out-of-Band Zero-Day Security Flaw for IE." *eWeek* (December 20, 2018).

Kwon, Juhee, and M. Eric Johnson."Meaningful Healthcare Security: Does Meaningful-Use Attestation Improve Information Security Performance?" *MIS Quarterly* 42, No. 4 (Decmber 2018).

Liang, Huigang, Yajiong Xue, Alain Pinsonneault, and Yu "Andy" Wu. "What Users Do Besides Problem-Focused Coping When Facing IT Security Threats: An Emotion-Focused Coping Perspective." *MIS Quarterly* 43, No. 2 (June 2019).

McMillan, Robert. "How the Capital One Hacker Stole Reams of Unsecured Data from the Cloud." *Wall Street Journal* (August 4, 2019a).

_____. "Microsoft Announces a Monster Computer Bug in a Week of Them." *Wall Street Journal* (May 15, 2019b).

Menard, Philip, Gregory J. Bott, and Robert E. Crossler. "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory." *Journal of Management Information Systems* 34, No. 4 (2017).

Moody, Gregory D., Mikko Siponen, and Seppo Pahnila. "Toward a Unified Model of Information Security Policy Compliance." *MIS Quarterly* 42, No. 1 (March 2018).

Oracle and KPMG. "Oracle and KPMG Cloud Threat Report" (2019).

Panda Security. "Cybersecurity Predictions 2019" (2018).

Panko, Raymond R., and Julie L. Panko. *Business Data Networks and Security*, 11th ed. Upper Saddle River, NJ: Pearson (2019).

Ponemon Institute. "Ninth Annual Cost of Cybercrime Study" (March 6, 2019).

_____. "2018 Cost of Data Breach Study" (2018).

Rothrock, Ray A., James Kaplan, and Friso Van der Oord. "The Board's Role in Managing Cybersecurity Risks." *MIT Sloan Management Review* (Winter 2018).

Samtani, Sagar, Ryan Chinn, Hsinchun Chen, and Jay F. Nunamaker. "Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence." *Journal of Management Information Systems* 34, No. 4 (2017).

Symantec. "Internet Security Threat Report" (February 2019).

Venkatraman, Srinivasan, M. K. Cheung, Christy Lee, W. Y. Zach, Fred D. Davis, and Viswanath Venkatesh."The "Darth" Side of Technology Use: An Inductively Derived Typology of Cyberdeviance." *Journal of Management Information Systems* 35, No. 4 (2018).

Wang, Jingguo, Zhe Shan, Manish Gupta, and H. Raghav Rao. "A Longitudinal Study of Unauthorized Access Attempts on Information Systems: The Role of Opportunity Contexts." *MIS Quarterly* 43, No. 2 (June 2019).

Yin, Hao Hua Sun, Klaus Langenheldt, Mikkel Harlev, Raghava Rao Mukkamala, and Ravi Vatrapu. "Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain." *Journal of Management Information Systems* 36, No. 1 (2019).

Young, Carl S. "The Enemies of Data Security: Convenience and Collaboration." *Harvard Business Review* (February 11, 2015).

Yue, Wei T., Qiu-Hong Wang, and Kai-Lung Hui. "See No Evil, Hear No Evil? Dissecting the Impact of Online Hacker Forums." *MIS Quarterly* 43, No. 1 (March 2019).