

# Information Systems Management

**Part 4 addresses** the management of information systems security, development, and resources. We begin with security because of its great importance today. With the Internet, the interconnectivity of systems, and the rise of inter-organizational IS, security problems in one organization become security problems in connected organizations as well. As you've learned, the millions of dollars of damage that Target incurred was due to an interorganizational systems problem. You'll see how that affects PRIDE in the Chapter 10 opener.

While you can readily understand that IS security is important to you as a future manager, it may be more difficult for you to appreciate why you need to know about IS development. As a business professional, you will be the customer of development projects. You need basic knowledge of development processes to be able to assess the quality of the work being done on your behalf. As a manager, you may allocate budget and release funds for IS development. You need knowledge that allows you to be an active and effective participant in such projects.

Finally, you need to know how IS resources are managed so that you can better relate to your IS department. IS managers can sometimes seem rigid and overly protective of IS assets, but usually they have important reasons for their concerns. You need to understand the IS department's perspective and know both your rights and responsibilities as a user of IS resources within your organization. Having such knowledge is key to success for any business professional today.

## Collaboration



FBA

Office 365

Jobs!

Google+ vs. Facebook

# Information Systems Security

CHAPTER

10

**James and Michele** are videoconferencing with Sam Ide, the manager of security for San Diego Sports, a large sports equipment vendor that Michele wants to involve in race events. Mr. Ide's job is to determine if PRIDE Systems provides an acceptable level of security. Michele has gone over this several times with San Diego Sports personnel, and they asked to speak with someone outside of sales who has direct knowledge of PRIDE Systems' security. Michele asked James to participate in the videoconference with Mr. Ide.

"Sam, I have James Wu, our IS manager here, on our videoconference line. Why don't I let you explain your concerns and I'll ask James to respond?"

"Sure. James, thanks for taking the time to speak with me."

"Happy to do it, Mr. Ide."

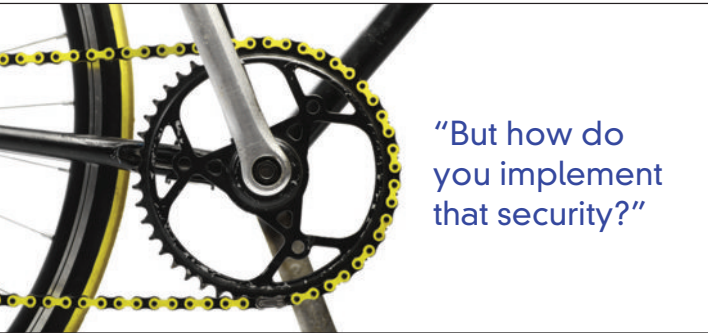
"Please, call me Sam. OK, we at SDS... that's how we refer to ourselves... we at SDS have always been concerned with security. But, given the recent troubles at Target and Adobe, our senior management team has asked us to be even more careful. It appears that criminals have begun to focus attacks on interorganizational systems, and so we address security with all of our partners."

"I understand, Sam. Although in this case, we're not talking about any connection between your systems and ours. As I understand it, we just want to feature San Diego Sports in a major way in our advertising and promotion of events." James is careful as he gains a sense of his interests.

"Thanks, James, that's my understanding as well. All the same, we don't want to become affiliated in the mind of our market with any company that does have a major security problem, and that's the reason for this call."

"Got it. Do you have specific matters you'd like me to address?"





**“But how do you implement that security?”**

Source: Bizoo\_n/iStock/Thinkstock/Getty Images

“Actually, I do. Michele has explained to me the basics of your security program, and she said that, given the fact that your systems were originally designed to store medical data, you have designed security deep into your systems.” Sam sounds like he’s reading from notes.

“Correct.” James nods at Michele as he says this.

“I wonder if you could explain that to me with some specifics.”

“Sure, but first, may I ask if you have a technical background?” James isn’t sure how much detail to provide him.

“I’m not a developer, not by a long shot, but I was closely involved as a systems analyst in the development of many of our systems.” Sam’s actually quite a bit more technical than he reveals.

“Great. Let me dive in then, and if the dive is too deep, just let me know.” There’s not the least bit of condescension in James’s voice as he speaks.

“Will do.”

“Each user is in charge of the distribution of his or her data. Initially, users’ data is not shared at all. But we provide a simple-to-use UI that allows users to change their security settings.”

“OK. Michele told me that. But how do you implement that security?” Sam wants to dive deeper.

“Because we have thousands and thousands of users, we store all privacy settings in a database and we have elaborate security on that database that I can go into later, if you want.” James wants to focus on specific PRIDE features.

“Maybe. Just keep explaining.”

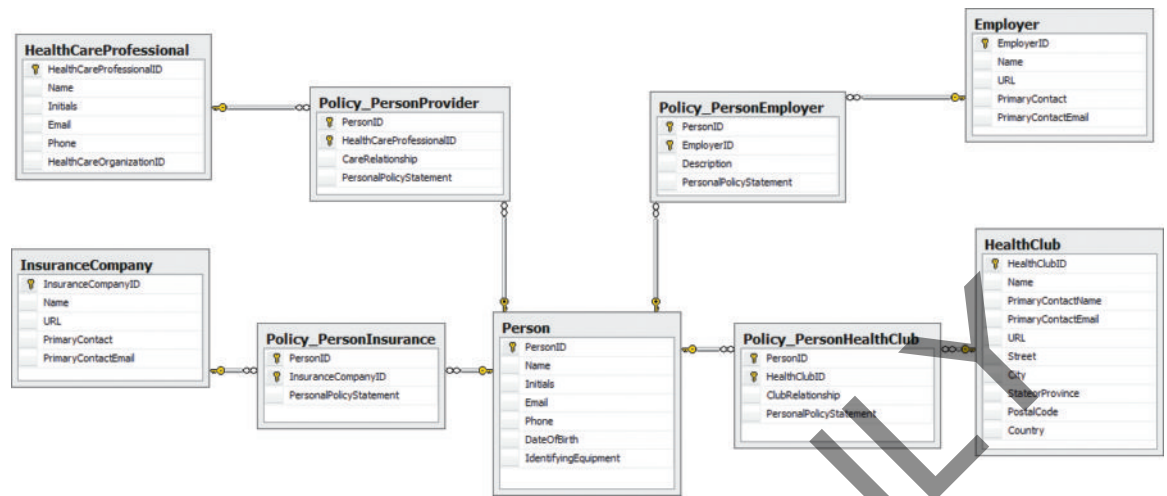
“It turns out that event participants have a many-to-many relationship with all of our major players. Thus, for example, a participant may belong to several health clubs, and of course a health club has a relationship to many of our participants. Similarly, a participant has a relationship to potentially many insurance companies, and each company can have a relationship to many of our participants. Are you with me?”

“Yes, keep going.” Sam sounds curious.

“So, as you know, to represent a many-to-many relationship we create an intersection or bridge table. And we store the security preferences for each person in his or her relationship to the external agent in that intersection table.”

## STUDY QUESTIONS

- Q1** What is the goal of information systems security?
- Q2** How big is the computer security problem?
- Q3** How should you respond to security threats?
- Q4** How should organizations respond to security threats?
- Q5** How can technical safeguards protect against security threats?
- Q6** How can data safeguards protect against security threats?
- Q7** How can human safeguards protect against security threats?
- Q8** How should organizations respond to security incidents?
- Q9** 2025?



Michele jumps in at this point. “Sam, let me see if I can bring up an illustration onto your screen. Do you see the table diagram?”

“Just a second. Something’s loading. Ah, yes, there it is.”

James continues, “OK, the data for each participant is stored in the Person table in the center. Actually, we store quite a bit more data than shown here, but this will give you the idea of what we do. The security allowed is stored in attributes called *PolicyStatements* in the intersection tables. By default, the value is ‘None.’ However, if someone decides to share his or her data with, say, a health club, then he or she uses a form to specify what he or she wants, and we store the result of that decision in the *PolicyStatement* attribute. All of our code uses the value of that attribute to limit data access.”

“That makes sense, it’s a clean design. But what about SQL injection?”

“Good question. There are four types of access allowed: None, which is the default; Non-identifying; Summary; and Full Access. The last two include the person’s identity. In the form, those four are presented with radio buttons and the user picks. There’s no place for SQL injection to occur.”

The meeting continues in this vein for another 15 minutes. Sam seems satisfied with James’s responses. Afterward, James and Michele walk back to their offices together.

“James, that was the best meeting I’ve had with him. He’s so impatient with me, but he related to you really well.”

“Michele, I’m glad you’re happy with it. I couldn’t tell what he thought, but his questions were good and ones that we’ve thought about a lot.”

“Well, James, you’re good at explaining things. Ever think about going into sales?”

“Heavens, no, Michele. But I’ll take that as a compliment.”

“Thanks again.”

## CHAPTER PREVIEW

This chapter provides an overview of the major components of information systems security. We begin in Q1 by defining the goals of IS security and then, in Q2, discuss the size of the computer security problem. Next, in Q3, we address how you, both as a student today and as a business professional in the future, should respond to security threats. Then, in Q4, we ask what organizations need to do to respond to



security threats. After that, Q5 through Q7 address security safeguards. Q5 discusses technical safeguards that involve hardware and software components, Q6 addresses data safeguards, and Q7 discusses human safeguards that involve procedure and people components. Q8 then summarizes what organizations need to do when they incur a security incident, and we wrap up the chapter with a preview of IS security in 2025.

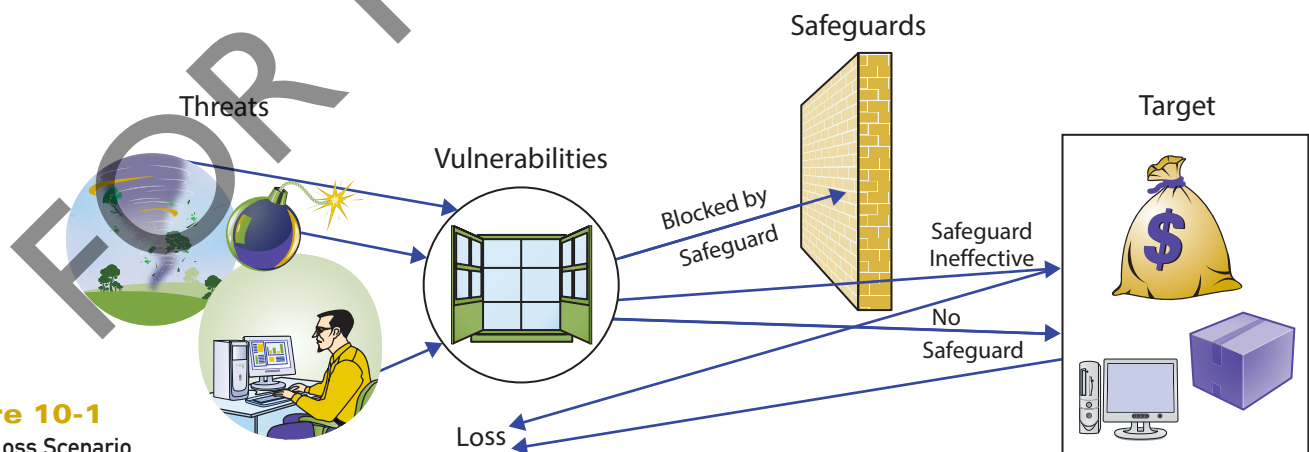
Unfortunately, threats to data and information systems are increasing and becoming more complex. In fact, the U.S. Bureau of Labor Statistics estimates that demand for security specialists will increase by more than 37 percent between 2012 and 2022 with a median salary of \$86,170. This is strong growth considering computer occupations are projected to grow at 18 percent and all occupations at 11 percent.<sup>1</sup> If you find this topic attractive, majoring in information systems with a security specialty would open the door to many interesting jobs.

## Q1 What Is the Goal of Information Systems Security?

Information systems security involves a trade-off between cost and risk. To understand the nature of this trade-off, we begin with a description of the security threat/loss scenario and then discuss the sources of security threats. Following that, we'll state the goal of information systems security.

### The IS Security Threat/Loss Scenario

Figure 10-1 illustrates the major elements of the security problem that individuals and organizations confront today. A **threat** is a person or organization that seeks to obtain or alter data or other IS assets illegally, without the owner's permission and often without the owner's knowledge. A **vulnerability** is an opportunity for threats to gain access to individual or organizational assets. For example, when you buy something online, you provide your credit card data; when that data is transmitted over the Internet, it is vulnerable to threats. A **safeguard** is some measure that individuals or organizations take to block the threat from obtaining the asset. Notice in Figure 10-1 that safeguards are not always effective; some threats achieve their goal despite safeguards. Finally, the **target** is the asset that is desired by the threat.



**Figure 10-1**  
Threat/Loss Scenario

<sup>1</sup>Bureau of Labor Statistics, U.S. Department of Labor, *2014–2015 Occupational Outlook Handbook*, accessed June 6, 2014, [www.bls.gov/ooh/](http://www.bls.gov/ooh/). Information about information security analysts can be found in the Computer and Information Technology section.

Threat/Target	Vulnerability	Safeguard	Result	Explanation
Hacker wants to steal your bank login credentials	Hacker creates a phishing site nearly identical to your online banking site	Only access sites using https	No loss	Effective safeguard
		None	Loss of login credentials	Ineffective safeguard
Employee posts sensitive data to public Google + group	Public access to not-secure group	Passwords Procedures Employee training	Loss of sensitive data	Ineffective safeguard

**Figure 10-2**  
Examples of Threat/Loss

Figure 10-2 shows examples of threats/targets, vulnerabilities, safeguards, and results. In the first two rows, a hacker (the threat) wants your bank login credentials (the target) to access your bank account. If you click on links in emails you can be directed to phishing sites that look identical to your bank's Web site. Phishing sites don't typically use https. If, as shown in the first row of Figure 10-2, you always access your bank's site using https rather than http (discussed in Q5), you will be using an effective safeguard, and you will successfully counter the threat.

If, however, as described in the second row of Figure 10-2, you access what appears to be your bank's site without using https (i.e., an unsecured site), you have no safeguard at all. Your login credentials can be quickly recorded and resold to other criminals.

The bottom row of Figure 10-2 shows another situation. Here an employee at work obtains sensitive data and posts it on what he thinks is a work-only Google+ group. However, the employee errs and instead posts it to a public group. The target is the sensitive data, and the vulnerability is public access to the group. In this case, there are several safeguards that should have prevented this loss; the employee needed passwords to obtain the sensitive data and to join the private, work-only group. The employer has procedures that state employees are not to post confidential data to any public site, such as Google+, but these procedures were either unknown or ignored. A third safeguard is the training that all employees are given. Because the employee ignores the procedures, though, all of those safeguards are ineffective and the data is exposed to the public.

## What Are the Sources of Threats?

Figure 10-3 summarizes the sources of security threats. The type of threat is shown in the columns, and the type of loss is shown in the rows.

### Human Error

*Human errors and mistakes* include accidental problems caused by both employees and non-employees. An example is an employee who misunderstands operating procedures and accidentally deletes customer records. Another example is an employee who, in the course of backing up a database, inadvertently installs an old database on top of the current one. This category also includes poorly written application programs and poorly designed procedures. Finally, human errors and mistakes include physical accidents, such as driving a forklift through the wall of a computer room.

### Computer Crime

The second threat type is *computer crime*. This threat type includes employees and former employees who intentionally destroy data or other system components. It also includes hackers who break into a system and virus and worm writers who infect computer systems. Computer crime also includes terrorists and those who break into a system to steal for financial gain.

		Threat		
		Human Error	Computer Crime	Natural Disasters
Loss	Unauthorized data disclosure	Procedural mistakes	Pretexting Phishing Spoofing Sniffing Hacking	Disclosure during recovery
	Incorrect data modification	Procedural mistakes Incorrect procedures Ineffective accounting controls System errors	Hacking	Incorrect data recovery
	Faulty service	Procedural mistakes Development and installation errors	Usurpation	Service improperly restored
	Denial of service (DoS)	Accidents	DoS attacks	Service interruption
	Loss of infrastructure	Accidents	Theft Terrorist activity	Property loss

**Figure 10-3**  
Security Problems and Sources

### Natural Events and Disasters

*Natural events and disasters* are the third type of security threat. This category includes fires, floods, hurricanes, earthquakes, tsunamis, avalanches, and other acts of nature. Problems in this category include not only the initial loss of capability and service, but also losses stemming from actions to recover from the initial problem.

### What Types of Security Loss Exist?

Five types of security loss exist: unauthorized data disclosure, incorrect data modification, faulty service, denial of service, and loss of infrastructure. Consider each.

#### Unauthorized Data Disclosure

*Unauthorized data disclosure* occurs when a threat obtains data that is supposed to be protected. It can occur by human error when someone inadvertently releases data in violation of policy. An example at a university is a department administrator who posts student names, identification numbers, and grades in a public place, when the releasing of names and grades violates state law and Federal law. Another example is employees who unknowingly or carelessly release proprietary data to competitors or to the media. WikiLeaks is a famous example of unauthorized disclosure; the situation described in the third row of Figure 10-2 is another example.

The popularity and efficacy of search engines have created another source of inadvertent disclosure. Employees who place restricted data on Web sites that can be reached by search engines might mistakenly publish proprietary or restricted data over the Web.

Of course, proprietary and personal data can also be released and obtained maliciously. **Pretexting** occurs when someone deceives by pretending to be someone else. A common scam involves a telephone caller who pretends to be from a credit card company and claims to be checking the validity of credit card numbers: "I'm checking your MasterCard number; it begins with 5491. Can you verify the rest of the number?" Thousands of MasterCard numbers start with 5491; the caller is attempting to steal a valid number.

*Phishing compromises legitimate brands and trademarks. See the Guide (pages 420–421) for more.*

**Phishing** is a similar technique for obtaining unauthorized data that uses pretexting via email. The **phisher** pretends to be a legitimate company and sends an email requesting confidential data, such as account numbers, Social Security numbers, account passwords, and so forth.

**Spoofing** is another term for someone pretending to be someone else. If you pretend to be your professor, you are spoofing your professor. **IP spoofing** occurs when an intruder uses another site's IP address to masquerade as that other site. **Email spoofing** is a synonym for phishing.

**Sniffing** is a technique for intercepting computer communications. With wired networks, sniffing requires a physical connection to the network. With wireless networks, no such connection is required: **Wardrivers** simply take computers with wireless connections through an area and search for unprotected wireless networks. They can monitor and intercept traffic on unsecured wireless networks. Even protected wireless networks are vulnerable, as you will learn. Spyware and adware are two other sniffing techniques discussed later in this chapter.

Other forms of computer crime include **hacking**, which is breaking into computers, servers, or networks to steal data such as customer lists, product inventory data, employee data, and other proprietary and confidential data.

Finally, people might inadvertently disclose data during recovery from a natural disaster. During a recovery, everyone is so focused on restoring system capability that they might ignore normal security safeguards. A request such as "I need a copy of the customer database backup" will receive far less scrutiny during disaster recovery than at other times.

### Incorrect Data Modification

The second type of security loss in Figure 10-3 is *incorrect data modification*. Examples include incorrectly increasing a customer's discount or incorrectly modifying an employee's salary, earned days of vacation, or annual bonus. Other examples include placing incorrect information, such as incorrect price changes, on a company's Web site or company portal.

Incorrect data modification can occur through human error when employees follow procedures incorrectly or when procedures have been designed incorrectly. For proper internal control on systems that process financial data or control inventories of assets, such as products and equipment, companies should ensure separation of duties and authorities and have multiple checks and balances in place.

A final type of incorrect data modification caused by human error includes *system errors*. An example is the lost-update problem discussed in Chapter 5 (page 178).

Computer criminals can make unauthorized data modifications by hacking into a computer system. For example, hackers could hack into a system and transfer people's account balances or place orders to ship goods to unauthorized locations and customers.

Finally, faulty recovery actions after a disaster can result in incorrect data changes. The faulty actions can be unintentional or malicious.

### Faulty Service

The third type of security loss, *faulty service*, includes problems that result because of incorrect system operation. Faulty service could include incorrect data modification, as just described. It also could include systems that work incorrectly by sending the wrong goods to a customer or the ordered goods to the wrong customer, inaccurately billing customers, or sending the wrong information to employees. Humans can inadvertently cause faulty service by making procedural mistakes. System developers can write programs incorrectly or make errors during the installation of hardware, software programs, and data.

**Usurpation** occurs when computer criminals invade a computer system and replace legitimate programs with their own, unauthorized ones that shut down legitimate applications and substitute their own processing to spy, steal and manipulate data, or achieve other purposes. Faulty service can also result when service is improperly restored during recovery from natural disasters.



## Denial of Service

Human error in following procedures or a lack of procedures can result in **denial of service (DoS)**, the fourth type of loss. For example, humans can inadvertently shut down a Web server or corporate gateway router by starting a computationally intensive application. An OLAP application that uses the operational DBMS can consume so many DBMS resources that order-entry transactions cannot get through.

Computer criminals can launch an intentional denial-of-service attack in which a malicious hacker floods a Web server, for example, with millions of bogus service requests that so occupy the server that it cannot service legitimate requests. Also, computer worms can infiltrate a network with so much artificial traffic that legitimate traffic cannot get through. Finally, natural disasters may cause systems to fail, resulting in denial of service.

## Loss of Infrastructure

Many times, human accidents cause loss of infrastructure, the last loss type. Examples are a bulldozer cutting a conduit of fiber-optic cables and a floor buffer crashing into a rack of Web servers.

Theft and terrorist events also cause loss of infrastructure. For instance, a disgruntled, terminated employee might walk off with corporate data servers, routers, or other crucial equipment. Terrorist events also can cause the loss of physical plants and equipment.

Natural disasters present the largest risk for infrastructure loss. A fire, flood, earthquake, or similar event can destroy data centers and all they contain.

You may be wondering why Figure 10-3 does not include terms such as viruses, worms, and Trojan horses. The answer is that viruses, worms, and Trojan horses are techniques for causing some of the problems in the figure. They can cause a denial-of-service attack, or they can be used to cause malicious, unauthorized data access or data loss.

Finally, a new threat term has come into recent use. An **Advanced Persistent Threat (APT)** is a sophisticated, possibly long-running computer hack that is perpetrated by large, well-funded organizations such as governments. APTs can be a means to engage in cyberwarfare and cyber-espionage. Examples of APT are *Stuxnet* and *Flame*. *Stuxnet* is reputed to have been used to set back the Iranian nuclear program by causing Iranian centrifuges to malfunction. *Flame* is a large, complex computer program that is reputed to have hacked into computers and is said to operate as a cyberspy, capturing screen images, email, and text messages and even searching nearby smartphones using Bluetooth communication. Search the Internet for these terms to learn more. If you work in the military or for intelligence agencies, you will certainly be concerned, if not involved, with APTs. We return to this topic in Q9.

## Goal of Information Systems Security

As shown in Figure 10-1, threats can be stopped, or if not stopped, the costs of loss can be reduced by creating appropriate safeguards. Safeguards are, however, expensive to create and maintain. They also reduce work efficiency by making common tasks more difficult, adding additional labor expense. The goal of information security is to find an appropriate trade-off between the risk of loss and the cost of implementing safeguards.

Business professionals need to consider that trade-off carefully. In your personal life, you should certainly employ antivirus software. You should probably implement other safeguards that you'll learn about in Q3. Some safeguards, such as deleting browser cookies, will make using your computer more difficult. Are such safeguards worth it? You need to assess the risks and benefits for yourself.

Similar comments pertain to organizations, though they need to go about it more systematically. The bottom line is not to let the future unfold without careful analysis and action as indicated by that analysis. Get in front of the security problem by making the appropriate trade-off for your life and your business.

## Q2 How Big Is the Computer Security Problem?

We do not know the full extent of the financial and data losses due to computer security threats. Certainly, the losses due to human error are enormous, but few organizations compute those losses, and even fewer publish them. However, a recent security report by Verizon called 2013 “year of the retailer breach.” The number of user accounts stolen by hackers included Adobe 150 million, Target Corp. 98 million, LivingSocial 50 million, Evernote 50 million, Korea Credit Bureau 20 million, Facebook 6 million, Schnuck Markets 2.4 million, Vodafone 2 million, and Neiman Marcus 1.1 million.<sup>2</sup> These are only the companies that made the news and reported estimated losses.

Losses due to natural disasters are also enormous and impossible to compute. The 2011 earthquake in Japan, for example, shut down Japanese manufacturing, and losses rippled through the supply chain from the Far East to Europe and the United States. One can only imagine the enormous expense for Japanese companies as they restored their information systems.

Furthermore, no one knows the cost of computer crime. For one, there are no standards for tallying crime costs. Does the cost of a denial-of-service attack include lost employee time, lost revenue, or long-term revenue losses due to lost customers? Or, if an employee loses a \$2,000 laptop, does the cost include the value of the data that was on it? Does it include the cost of the time of replacing it and reinstalling software? Or, if someone steals next year’s financial plan, how is the cost of the value that competitors glean determined?

Second, all the studies on the cost of computer crime are based on surveys. Different respondents interpret terms differently, some organizations don’t report all their losses, and some won’t report computer crime losses at all. Absent standard definitions and a more accurate way of gathering crime data, we cannot rely on the accuracy of any particular estimate. The most we can do is look for trends by comparing year-to-year data, assuming the same methodology is used by the various types of survey respondents.

Figure 10-4 shows the results of a survey done over four years.<sup>3</sup> It was commissioned by Hewlett-Packard and performed by the Ponemon Institute, a consulting group that specializes in computer crime. As shown, the study estimated the median loss per organization in 2013 to be \$9.1 million, more than double that in 2010. From this we can conclude that the cost of crime for most organizations is increasing, but within bounds. Computer criminals aren’t taking more per incident, but they’re taking more from more organizations.

By the way, this data underlines the problems of tallying crime data from surveys. In 2013, no organization reported less than \$1.3 million in loss. Clearly, the survey did not include small companies that incurred small losses. Given the large number of small companies, those unknown losses could be substantial.

Figure 10-5, from the same Ponemon study, shows the average cost and percent of total incidents of the six most expensive types of attack. Without tests of significance, it’s difficult to determine if the differences shown are random; they could be. But, taking the data at face value,

**Figure 10-4**  
Computer Crime Costs per Organizational Respondent (Worldwide, in Millions of U.S. Dollars)

Source: Ponemon Institute. *2013 Cost of Cyber Crime Study: United States*, October 2013, p. 5.

	2010	2011	2012	2013
Maximum	\$51.9	\$36.5	\$46.0	\$58.1
Median	\$3.8	\$5.9	\$6.2	\$9.1
Minimum	\$1.0	\$1.5	\$1.4	\$1.3

<sup>2</sup>Verizon 2014 Data Breach Investigations Report, accessed June 2014, [www.verizonenterprise.com/DBIR/2014/](http://www.verizonenterprise.com/DBIR/2014/).

<sup>3</sup>Ponemon Institute, *2013 Cost of Cyber Crime Study: United States*. October 2013.

	2010	2011	2012	2013
Denial of Service	NA	\$187,506 (17%)	\$172,238 (20%)	\$243,913 (21%)
Malicious Insiders	\$100,300 (11%)	\$105,352 (9%)	\$166,251 (8%)	\$198,769 (8%)
Web-based Attacks	\$143,209 (15%)	\$141,647 (12%)	\$125,795 (13%)	\$125,101 (12%)
Malicious Code	\$124,083 (26%)	\$126,787 (23%)	\$109,533 (26%)	\$102,216 (21%)
Phishing and Social Engineering	\$35,514 (12%)	\$30,397 (9%)	\$18,040 (7%)	\$21,094 (11%)
Stolen Devices	\$25,663 (17%)	\$24,968 (13%)	\$23,541 (12%)	\$20,070 (9%)

**Figure 10-5**  
Average Computer Crime Cost and Percent of Attacks by Type (6 Most Expensive Types)

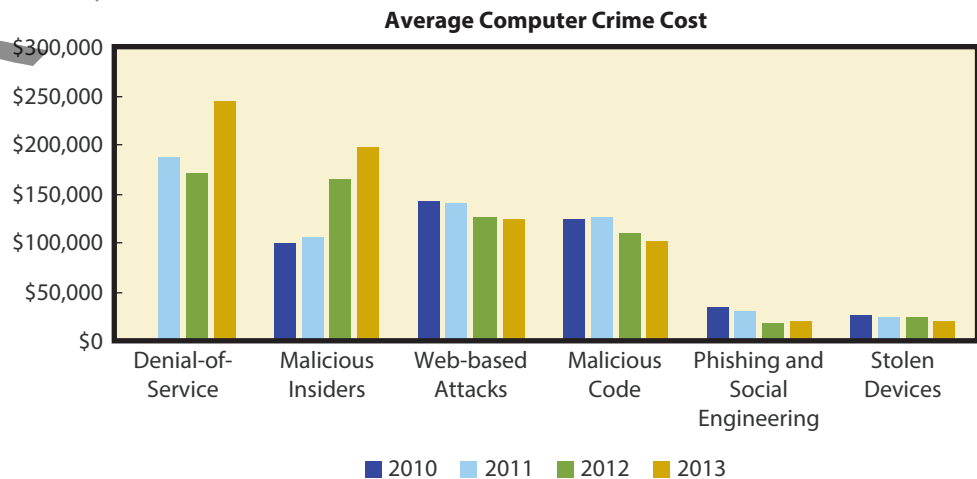
Source: Ponemon Institute. *2013 Cost of Cyber Crime Study: United States*, October 2013, p. 12.

it appears the source of most of the increase in computer crime costs is malicious insiders. The number of attacks of this type is slightly decreasing, but the average cost of such attacks is increasing, possibly dramatically (Figure 10-6). Apparently, insiders are getting better at stealing more. The study, by the way, defined an insider as an employee, temporary employee, contractor, or business partner. The average costs of the remaining categories are slightly decreasing.

In addition to this data, Ponemon also surveyed losses by type of asset compromised. It found that data loss was the single most expensive consequence of computer crime, accounting for 43 percent of costs in 2013. Business disruption was the second highest cost, at 36 percent in 2013. Equipment losses and damages were only 4 percent of the lost value. Clearly, value lies in data and not in hardware!

Looking to the future, in a separate study,<sup>4</sup> Ponemon reported that 80 percent of its respondents believe that the data on mobile devices poses significant risks to their organizations and 73 percent reported that this threat was greater in 2012 than it was in 2011. The second most worrisome concern was Advanced Persistent Threats.

The *2013 Cost of Computer Crime Study* includes an in-depth analysis of the effect of different security policies on the savings in computer crime. The bottom line is that organizations



**Figure 10-6**  
Computer Crime Costs

<sup>4</sup>Ponemon Institute, *2013 State of the EndPoint*, December 2012.

that spend more to create the safeguards discussed in Q4–Q7 (later in this chapter) experience less computer crime and suffer smaller losses when they do. Security safeguards do work!

If you search for the phrase *computer crime statistics* on the Web, you will find numerous similar studies. Many are based on dubious sampling techniques, and some seem to be written to promote a particular safeguard product or point of view. Be aware of such bias as you read.

Using the Ponemon study, the bottom line, as of 2013, is:

- The median average cost of computer crime is increasing.
- Malicious insiders are an increasingly serious security threat.
- Data loss is the principal cost of computer crime.
- Survey respondents believe mobile device data is a significant security threat.
- Security safeguards work.

## Q3 How Should You Respond to Security Threats?

As stated at the end of Q1, your personal IS security goal should be to find an effective trade-off between the risk of loss and the cost of safeguards. However, few individuals take security as seriously as they should, and most fail to implement even low-cost safeguards.

Figure 10-7 lists recommended personal security safeguards. The first safeguard is to take security seriously. You cannot see the attempts that are being made, right now, to compromise your computer. However, they are there.

Unfortunately, the first sign you receive that your security has been compromised will be bogus charges on your credit card or messages from friends complaining about the disgusting email they just received from your email account. Computer security professionals run intrusion detection systems to detect attacks. An **intrusion detection system (IDS)** is a computer program that senses when another computer is attempting to scan or access a computer or network. IDS logs can record thousands of attempts each day. If these attempts come from outside the country, there is nothing you can do about them except use reasonable safeguards.

If you decide to take computer security seriously, the single most important safeguard you can implement is to create and use strong passwords. We discussed ways of doing this in Chapter 1 (pages 24–25). To summarize, do not use any word, in any language, as part of your password. Use passwords with a mixture of upper- and lowercase letters and numbers and special characters.

Such nonword passwords are still vulnerable to a **brute force attack** in which the password cracker tries every possible combination of characters. John Pozadzides, a security researcher, estimates that a brute force attack can crack a six-character password of either upper- or

- Take security seriously
- Create strong passwords
- Use multiple passwords
- Send no valuable data via email or IM
- Use https at trusted, reputable vendors
- Remove high-value assets from computers
- Clear browsing history, temporary files, and cookies (CCleaner or equivalent)
- Regularly update antivirus software
- Demonstrate security concern to your fellow workers
- Follow organizational security directives and guidelines
- Consider security for all business initiatives

**Figure 10-7**  
Personal Security Safeguards

lowercase letters in about 5 minutes. However, brute force requires 8.5 days to crack that length password having a mixture of upper- and lowercase letters, numbers, and special characters. A 10-digit password of only upper- and lowercase letters takes 4.5 years to crack, but one using a mix of letters, numbers, and special characters requires nearly 2 million years. A 12-digit, letter-only password requires 3 million years, and a 12-digit mixed password will take many, many millions of years.<sup>5</sup> All of these estimates assume, of course, that the password contains no word in any language. The bottom line is this: Use long passwords with no words, 10 or more characters, and a mix of letters, numbers, and special characters.

In addition to using long, complex passwords, you should also use different passwords for different sites. That way, if one of your passwords is compromised, you do not lose control of all of your accounts. Make sure you use very strong passwords for important sites (like your bank's site), and do not reuse those passwords on less important sites (like your social networking sites). Some sites are focused on innovating products and may not allocate the same amount of resources to protect your information. Guard your information with a password it deserves.

Never send passwords, credit card data, or any other valuable data in email or IM. As stated numerous times in this text, most email and IM is not protected by encryption (see Q5), and you should assume that anything you write in email or IM could find its way to the front page of *The New York Times* tomorrow.

Buy only from reputable online vendors using a secure https connection. If the vendor does not support https in its transactions (look for *https://* in the address line of your browser), do not buy from that vendor.

You can reduce your vulnerability to loss by removing high-value assets from your computers. Now, and especially later as a business professional, make it your practice not to travel out of your office with a laptop or other device that contains any data that you do not need. In general, store proprietary data on servers or removable devices that do not travel with you. (Office 365, by the way, uses https to transfer data to and from SharePoint. You can use it or a similar application for processing documents from public locations such as airports while you are traveling.)

Your browser automatically stores a history of your browsing activities and temporary files that contain sensitive data about where you've visited, what you've purchased, what your account names and passwords are, and so forth. It also stores **cookies**, which are small files that your browser receives when you visit Web sites. Cookies enable you to access Web sites without having to sign in every time, and they speed up processing of some sites. Unfortunately, some cookies also contain sensitive security data. The best safeguard is to remove your browsing history, temporary files, and cookies from your computer and to set your browser to disable history and cookies.

CCleaner is a free, open source product that will do a thorough job of securely removing all such data (<http://download.cnet.com/ccleaner/>). You should make a backup of your computer before using CCleaner, however.

Removing and disabling cookies presents an excellent example of the trade-off between improved security and cost. Your security will be substantially improved, but your computer will be more difficult to use. You decide, but make a conscious decision; do not let ignorance of the vulnerability of such data make the decision for you.

We will address the use of antivirus software in Q5. The last three items in Figure 10-7 apply once you become a business professional. With your coworkers, and especially with those whom you manage, you should demonstrate a concern and respect for security. You should also follow all organizational security directives and guidelines. Finally, consider security in all of your business initiatives.

*Management sets security policies to ensure compliance with security law, as discussed in the Ethics Guide on pages 402–403.*

<sup>5</sup>John Pozadzides, "How I'd Hack Your Weak Passwords." *One Man's Blog*, last modified March 26, 2007, <http://onemansblog.com/2007/03/26/how-id-hack-your-weak-passwords/>. When Pozadzides wrote this in 2007, it was for a personal computer. Using 2013 technology, these times would be half or less. Using a cloud-based network of servers for password cracking would cut these times by 90 percent or more.



SO WHAT?

# The Latest from Black Hat

Hackers, security professionals, and government agents flock to Las Vegas each year to attend an important security conference: Black Hat. Black Hat caters to hackers, security professionals, corporations, and government entities.

Each year speakers make briefings on how things can be hacked. Presenters show exactly how to exploit weaknesses in hardware, software, protocols, or systems. One session may show you how to hack your smartphone, while another may show you how to empty the cash out of an ATM.

Presentations encourage companies to fix product vulnerabilities and serve as an educational forum for hackers, developers, manufacturers, and government agencies. The following are highlights from the 2013 Black Hat conference:

**NSA Spying:** The most talked-about event was the keynote presentation by General Keith Alexander, director of the NSA. General Alexander explained how the NSA's PRISM program is used to thwart terrorist attacks.

He tried to convince an unbelieving audience that the NSA does not collect detailed information on U.S. citizens, but simply metadata like call times, duration, source, and carrier. Audience members heckled him, and few were convinced.<sup>6</sup> Many believe he appeared only because of the public outcry after Edward Snowden revealed the massive spy program a month earlier on June 5, 2013.<sup>7</sup> General Alexander announced his retirement a couple months later.

**Custom Spear-phishing:** Joaquim Espinhara and Ulisses Albuquerque showed how attackers use social media content (e.g., content from Twitter, Facebook, and Instagram) to craft custom spear-phishing emails.<sup>8</sup> These emails would model your same writing style and appear to come from a friend. The researchers showed their new application that creates a communication "fingerprint" for each user. Using this technology, emails can look and sound like messages from a friend, but actually be from a hacker on the other side of the world.



Source: Rawpixel/Fotolia

**Botnets from Browsers:** Matt Johanson, from WhiteHat Security, showed how JavaScript placed into a banner ad can make that computer part of a botnet and attack a victim.<sup>9</sup> As a test case, Johanson inserted some JavaScript into a generic banner ad and paid to have it submitted to several ad networks. When users were served the ad, the JavaScript in the banner ad started making repeated connections to a test server. The small ad generated more than 20 million hits. This type of attack could be used to target a legitimate server using a distributed denial-of-service (DDoS) attack.

**Hacking an iPhone:** Georgia Tech students Billy Lau, Yeongjin Jang, and Chengyu Song, showed how to hack an iPhone by plugging it into a special charging station.<sup>10</sup> Once plugged in, users just had to enter their passcode and the iPhone was compromised. An attacker could load malicious apps, read data, and take screenshots—all without permission. The researchers contacted Apple about patching iOS and cautioned users about using unknown charging stations.

<sup>6</sup>Fahmida Y. Rashid, "Black Hat 2013: NSA Chief Reveals Details About PRISM as Hecklers Call Him a Liar," *PCMag.com Security Watch*, August 2, 2013, accessed May 28, 2014, <http://securitywatch.pcmag.com/security/314333-black-hat-2013-nsa-chief-reveals-details-about-prism-as-hecklers-call-him-a-liar>.

<sup>7</sup>Matthew Cole and Mike Bruner, "Edward Snowden: A Timeline," NBC News, accessed May 28, 2014, [www.nbcnews.com/feature/edward-snowden-interview/edward-snowden-timeline-n114871](http://www.nbcnews.com/feature/edward-snowden-interview/edward-snowden-timeline-n114871).

<sup>8</sup>Fahmida Y. Rashid, "Smart Bot Reads Your Facebook, Mimics You in Spear Phishing Messages," *PCMag.com Security Watch*, August 2, 2013, accessed May 28, 2014, <http://securitywatch.pcmag.com/security/314402-smart-bot-reads-your-facebook-mimics-you-in-spear-phishing-messages>.

<sup>9</sup>Sean Michael Kerner, "Black Hat: Ads Could Provide a Vehicle for Enslaving Your Browser," *eWeek*, July 31, 2013, accessed May 28, 2014, [www.eweek.com/security/black-hat-ads-could-provide-a-vehicle-for-enslaving-your-browser](http://www.eweek.com/security/black-hat-ads-could-provide-a-vehicle-for-enslaving-your-browser).

<sup>10</sup>Violet Blue, "Researchers Reveal How to Hack an iPhone in 60 seconds," *ZDNet*, July 31, 2013, accessed May 28, 2014, [www.zdnet.com/researchers-reveal-how-to-hack-an-iphone-in-60-seconds-7000018822](http://www.zdnet.com/researchers-reveal-how-to-hack-an-iphone-in-60-seconds-7000018822).

## Questions

1. Why would security personnel from government agencies (like the NSA) want to attend an annual security convention with hackers?
2. Would the NSA or other security firms want to hire hackers from Black Hat? Why or why not?
3. Why does spying done on U.S. citizens by the NSA bother people? Does it bother you or make you feel safer? Why?
4. Why would automated custom spear-phishing be so dangerous?
5. How might browser botnet armies be prevented?
6. Why do devices, operating systems, and applications begin to have more security issues as they become more popular?
7. It seems unlikely that everyone who finds a new security threat goes to Black Hat and presents it to the public. What are other options? How can knowledge of this possibility help you?

### Q4 How Should Organizations Respond to Security Threats?

Q3 discussed ways that you as an individual should respond to security threats. In the case of organizations, a broader and more systematic approach needs to be taken. To begin, senior management needs to address two critical security functions: security policy and risk management.

Considering the first, senior management must establish company-wide security policies. Take, for example, a data security policy that states the organization's posture regarding data that it gathers about its customers, suppliers, partners, and employees. At a minimum, the policy should stipulate:

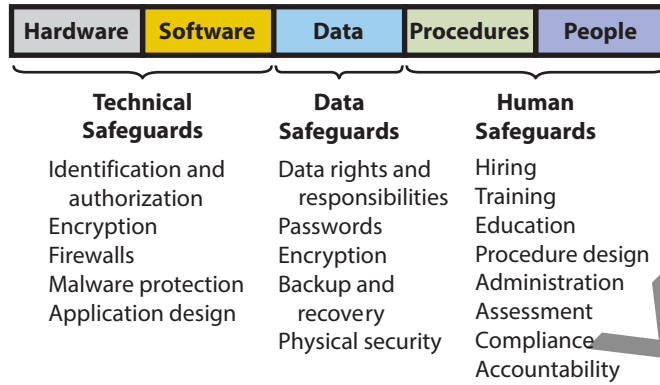
- What sensitive data the organization will store
- How it will process that data
- Whether data will be shared with other organizations
- How employees and others can obtain copies of data stored about them
- How employees and others can request changes to inaccurate data

The specifics of a policy depend on whether the organization is governmental or nongovernmental, on whether it is publically held or private, on the organization's industry, on the relationship of management to employees, and on other factors. As a new hire, seek out your employer's security policy if it is not discussed with you in new-employee training.

The second senior management security function is to manage risk. Risk cannot be eliminated, so *manage risk* means to proactively balance the trade-off between risk and cost. This trade-off varies from industry to industry and from organization to organization. Financial institutions are obvious targets for theft and must invest heavily in security safeguards. On the other hand, a bowling alley is unlikely to be much of a target, unless, of course, it stores credit card data on computers or mobile devices (a decision that would be part of its security policy and that would seem unwise, not only for a bowling alley but also for most small businesses).

To make trade-off decisions, organizations need to create an inventory of the data and hardware they want to protect and then evaluate safeguards relative to the probability of each potential threat. Figure 10-3 is a good source for understanding categories and frequencies of threat. Given this set of inventory and threats, the organization needs to decide how much risk it wishes to take or, stated differently, which security safeguards it wishes to implement.

A good analogy of using safeguards to protect information assets is buying car insurance. Before buying car insurance you determine how much your car is worth, the likelihood of



**Figure 10-8**  
Security Safeguards as They Relate to the Five Components

incurring damage to your car, and how much risk you are willing to accept. Then you transfer some of your risk to the insurer by buying a safeguard called an insurance policy. Instead of buying just one insurance policy, organizations implement a variety of safeguards to protect their data and hardware.

An easy way to remember information systems safeguards is to arrange them according to the five components of an information system, as shown in Figure 10-8. Some of the safeguards involve computer hardware and software. Some involve data; others involve procedures and people. We will consider technical, data, and human safeguards in the next three questions.

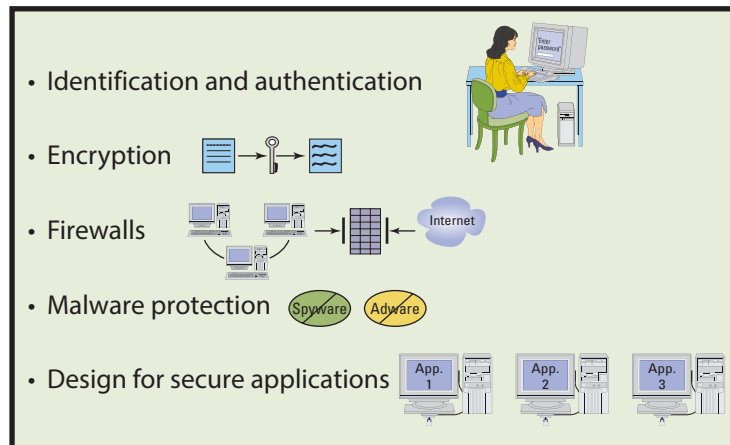
## Q5 How Can Technical Safeguards Protect Against Security Threats?

**Technical safeguards** involve the hardware and software components of an information system. Figure 10-9 lists primary technical safeguards. Consider each.

### Identification and Authentication

Every information system today should require users to sign on with a username and password. The username *identifies* the user (the process of **identification**), and the password *authenticates* that user (the process of **authentication**).

Passwords have important weaknesses. In spite of repeated warnings (don't let this happen to you!), users often share their passwords, and many people choose ineffective, simple passwords. In fact, a 2014 Verizon report states, "Passwords, usernames, emails, credit/debit card and financial



**Figure 10-9**  
Technical Safeguards

# Ethics Guide

## SECURING PRIVACY

**Some organizations** have legal requirements to protect the customer data they collect and store, but the laws may be more limited than you think. The **Gramm-Leach-Bliley (GLB) Act**, passed by Congress in 1999, protects consumer financial data stored by financial institutions, which are defined as banks, securities firms, insurance companies, and organizations that supply financial advice, prepare tax returns, and provide similar financial services.

The **Privacy Act of 1974** provides protections to individuals regarding records maintained by the U.S. government, and the privacy provisions of the **Health Insurance Portability and Accountability Act (HIPAA)** of 1996 give individuals the right to access health data created by doctors and other healthcare providers. HIPAA also sets rules and limits on who can read and receive your health information.

The law is stronger in other countries. In Australia, for example, the Privacy Principles of the Australian Privacy Act of 1988 govern not only government and healthcare data, but also records maintained by businesses with revenues in excess of AU\$3 million.

Most consumers would say, however, that online retailers have an ethical requirement to protect a customer's credit card and other data, and most online retailers would agree. Or at least the retailers would agree that they have a strong business reason to protect that data. A substantial loss of credit card data by any large online retailer would have detrimental effects on both sales and brand reputation.

Data aggregators like Acxiom Corporation further complicate the risk to individuals because they develop a complete profile of households and individuals. And no federal law prohibits the U.S.

government from buying information products from the data accumulators.

But let's bring the discussion closer to home. What requirements does your university have on the data it maintains about you? State law or university policy may govern those records, but no federal law does. Most universities consider it their responsibility to provide public access to graduation records. Anyone can determine when you graduated, your degree, and your major. (Keep this service in mind when you write your resume.)

Most professors endeavor to publish grades by student number and not by name, and there may be state law that requires that separation. But what about your work? What about the papers you write, the answers you give on exams? What about the emails you send to your professor? The data are not protected by federal law, and they are probably not protected by state law. If your professor chooses to cite your work in research, she will be subject to copyright law, but not privacy law. What you write is no longer your personal property; it belongs to the academic community. You can ask your professor what she intends to do with your coursework, emails, and office conversations, but none of these data are protected by law.



Source: Mopic/Fotolia

The bottom line is this: Be careful where you put your personal data. Large, reputable organizations are likely to endorse ethical privacy policy and to have strong and

effective safeguards to effectuate that policy. But individuals and small organizations might not. If in doubt, don't give the data.



## DISCUSSION QUESTIONS

1. As stated in the case, when you order from an online retailer, the data you provide is not protected by U.S. privacy law. Does this fact cause you to reconsider setting up an account with a stored credit card number? What is the advantage of storing the credit card number? Do you think the advantage is worth the risk? Are you more willing to take the risk with some companies than with others? If so, state the criteria you use for choosing to take the risk.
2. Suppose you are the treasurer of a student club and you store records of club members' payments in a database. In the past, members have disputed payment amounts; therefore, when you receive a payment, you scan an image of the check or credit card invoice and store the scanned image in a database. Unfortunately, you have placed that database into a shared folder. (See the Security Guide in Chapter 12, pages 492–493.)

One day, you are using your computer in a local coffee shop. A malicious student watches you sign in. Your name is visible, and your password is very short so it's easy for that student to see what it is. While you're enjoying your coffee, the malicious student learns the name of your computer from the coffee shop's wireless device, uses your login and password to connect to your shared folder, and then copies the club database. You know nothing about this until the next day, when a club member complains that a popular student Web site has published the names, bank names, and bank account numbers for everyone who has given you a check.

What liability do you have in this matter? Could you be classified as a financial institution because you are taking students' money? (You can find the GLB at [www.ftc.gov/privacy/privacyinitiatives/glbact.html](http://www.ftc.gov/privacy/privacyinitiatives/glbact.html).) If so, what liability do you have? If not, do you have any other liability? Does the coffee shop have liability?

Even if you have no legal liability, was your behavior ethical? Explain your answer. In this and in questions 3, 4, and 5, use either the categorical imperative or utilitarianism in your answer.
3. Suppose you are asked to fill out a study questionnaire that requires you to enter identifying data, as well as answers to personal questions. You hesitate to provide the data, but the top part of the questionnaire states, "All responses will be strictly confidential." So, you fill out the questionnaire.

Unfortunately, the person who is managing the study visits that same wireless coffee shop that you visited (in question 2), but this time the malicious student is sniffing packets to see what might turn up.

The study manager joins the coffee shop's wireless network and starts her email. Her first message is from a small online Web store at which she has just opened an account. The email says, in part, "Welcome! Your account name is *Emily100* and your password is *Jd5478IaE\$%\$55*."

"Eureka!" says the packet-sniffing, malicious student to himself as the packets carrying that email appear on his screen. "That looks like a pretty good password. Well, *Emily100*, I'll bet you use it on other accounts, like maybe your email?" The malicious student signs into email using *Emily100* and password *Jd5478IaE\$%\$55* and, sure enough, he's in. First thing he reads are emails to the study monitors, emails that contain attachments containing all of the study results. The next day, your name and all of your "confidential" responses appear on the public student Web site.

Did the person conducting the study violate a law? Did she do anything unethical? What mistake(s) did she make?
4. In question 3, does the online Web site that sent the email have any legal liability for this loss? Did it do anything unethical?
5. In question 2, did the malicious student do anything illegal? Unethical? In question 3, did the malicious student do anything illegal? Unethical?
6. Given these two scenarios, describe good practice for computer use at public wireless facilities.
7. Considering your answers to the above questions, state three to five general principles to guide your actions as you disseminate and store data.



account information, and Social Security Numbers are being compromised at a staggering rate, endangering the identities of consumers nationwide."<sup>11</sup> Because of these problems, some organizations choose to use smart cards and biometric authentication in addition to passwords.

### Smart Cards

A **smart card** is a plastic card similar to a credit card. Unlike credit, debit, and ATM cards, which have a magnetic strip, smart cards have a microchip. The microchip, which holds far more data than a magnetic strip, is loaded with identifying data. Users of smart cards are required to enter a **personal identification number (PIN)** to be authenticated.

### Biometric Authentication

**Biometric authentication** uses personal physical characteristics such as fingerprints, facial features, and retinal scans to authenticate users. Biometric authentication provides strong authentication, but the required equipment is expensive. Often, too, users resist biometric identification because they feel it is invasive.

Biometric authentication is in the early stages of adoption. Because of its strength, it likely will see increased usage in the future. It is also likely that legislators will pass laws governing the use, storage, and protection requirements for biometric data. For more on biometrics, search for *biometrics* at <http://searchsecurity.techtarget.com>.

Note that authentication methods fall into three categories: what you know (password or PIN), what you have (smart card), and what you are (biometric).

### Single Sign-on for Multiple Systems

Information systems often require multiple sources of authentication. For example, when you sign on to your personal computer, you need to be authenticated. When you access the LAN in your department, you need to be authenticated again. When you traverse your organization's WAN, you will need to be authenticated to even more networks. Also, if your request requires database data, the DBMS server that manages that database will authenticate you yet again.

It would be annoying to enter a name and password for every one of these resources. You might have to use and remember five or six different passwords just to access the data you need to perform your job. It would be equally undesirable to send your password across all of these networks. The further your password travels, the greater the risk it can be compromised.

Instead, today's operating systems have the capability to authenticate you to networks and other servers. You sign on to your local computer and provide authentication data; from that point on your operating system authenticates you to another network or server, which can authenticate you to yet another network and server, and so forth. Because this is so, your identity and passwords open many doors beyond those on your local computer; remember this when you choose your passwords!

### Encryption

**Encryption** is the process of transforming clear text into coded, unintelligible text for secure storage or communication. Considerable research has gone into developing **encryption algorithms** (procedures for encrypting data) that are difficult to break. Commonly used methods are DES, 3DES, and AES; search the Web for these terms if you want to know more about them.

A **key** is a number used to encrypt the data. It is called a *key* because it unlocks a message, but it is a number used with an encryption algorithm and not a physical thing like the key to your apartment.

<sup>11</sup>Verizon 2014 Data Breach Investigations Report, accessed June 2014, [www.verizonenterprise.com/DBIR/2014/](http://www.verizonenterprise.com/DBIR/2014/).

To encrypt a message, a computer program uses the encryption method (say AES) combined with the key (say the word “key”) to convert a plaintext message (in this case the word “secret”) into an encrypted message. The resulting coded message (“U2FsdGVkX1+b637aTP80u+y2WYlUbqUz2XtYcw4E8m4=”) looks like gibberish. Decoding (decrypting) a message is similar; a key is applied to the coded message to recover the original text. With **symmetric encryption**, the same key (again, a number) is used to encode and to decode. With **asymmetric encryption**, two keys are used; one key encodes the message, and the other key decodes the message. Symmetric encryption is simpler and much faster than asymmetric encryption.

A special version of asymmetric encryption, **public key encryption**, is used on the Internet. With this method, each site has a *public key* for encoding messages and a *private key* for decoding them. Before we explain how that works, consider the following analogy.

Suppose you send a friend an open combination lock (like you have on your gym locker). Suppose you are the only one who knows the combination to that lock. Now, suppose your friend puts something in a box and locks the lock. Now, neither your friend nor anyone else can open that box. That friend sends the locked box to you, and you apply the combination to open the box.

A *public key* is like the combination lock, and the *private key* is like the combination. Your friend uses the public key to code the message (lock the box), and you use the private key to decode the message (use the combination to open the lock).

Now, suppose we have two generic computers, A and B. Suppose B wants to send an encrypted message to A. To do so, A sends B its public key (in our analogy, A sends B an open combination lock). Now B applies A’s public key to the message and sends the resulting coded message back to A. At that point, neither B nor anyone other than A can decode that message. It is like the box with a locked combination lock. When A receives the coded message, A applies its private key (the combination in our analogy) to unlock or decrypt the message.

Again, public keys are like open combination locks. Computer A will send a lock to anyone who asks for one. But A never sends its private key (the combination) to anyone. Private keys stay private.

Most secure communication over the Internet uses a protocol called **https**. With https, data are encrypted using a protocol called the **Secure Sockets Layer (SSL)**, which is also known as **Transport Layer Security (TLS)**. SSL/TLS uses a combination of public key encryption and symmetric encryption.

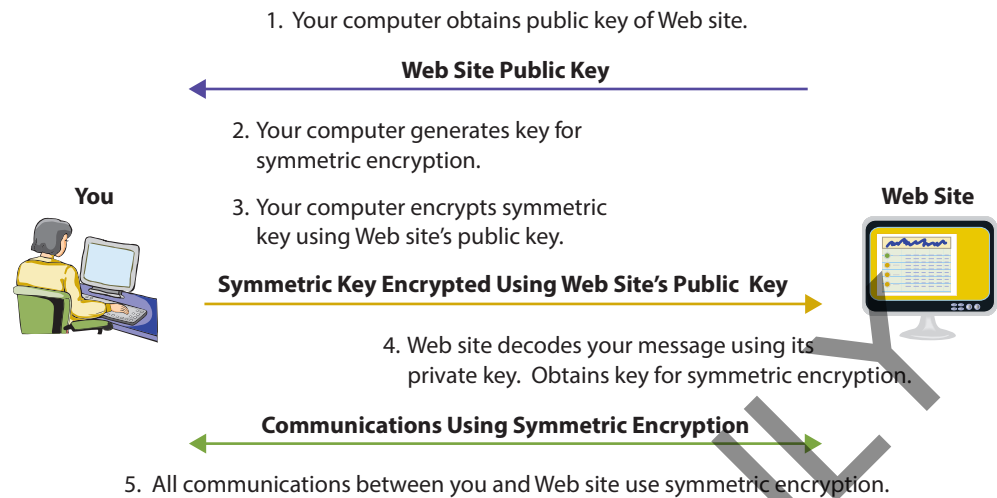
The basic idea is this: Symmetric encryption is fast and is preferred. But the two parties (say, you and a Web site) don’t share a symmetric key. So, the two of you use public key encryption to share the same symmetric key. Once you both have that key, you use symmetric encryption for the remainder of the communication.

Figure 10-10 summarizes how SSL/TLS works when you communicate securely with a Web site:

1. Your computer obtains the *public key* of the Web site to which it will connect.
2. Your computer generates a key for symmetric encryption.
3. Your computer encodes that key using the Web site’s public key. It sends the encrypted symmetric key to the Web site.
4. The Web site then decodes the symmetric key using its *private key*.
5. From that point forward, your computer and the Web site communicate using symmetric encryption.

At the end of the session, your computer and the secure site discard the keys. Using this strategy, the bulk of the secure communication occurs using the faster symmetric encryption. Also, because keys are used for short intervals, there is less likelihood they can be discovered.

Use of SSL/TLS makes it safe to send sensitive data such as credit card numbers and bank balances. Just be certain that you see *https://* in your browser and not just *http://*. Most browsers have additional plug-ins or add-ons (like HTTPS Everywhere) that can force https connections when available.

**Figure 10-10**

The Essence of https (SSL or TLS)

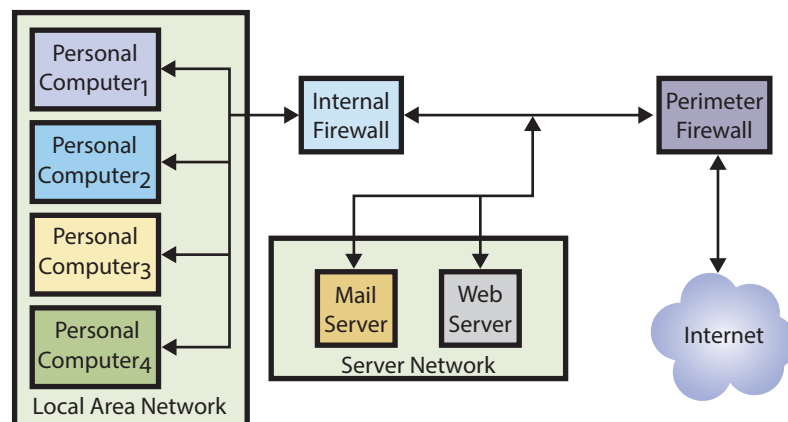
## Firewalls

A **firewall** is a computing device that prevents unauthorized network access. A firewall can be a special-purpose computer, or it can be a program on a general-purpose computer or on a router. In essence, a firewall is simply a filter. It can filter traffic in a variety of ways including where network traffic is coming from, what types of packets are being sent, the contents of the packets, and if the packets are part of an authorized connection.

Organizations normally use multiple firewalls. A **perimeter firewall** sits outside the organizational network; it is the first device that Internet traffic encounters. In addition to perimeter firewalls, some organizations employ **internal firewalls** inside the organizational network. Figure 10-11 shows the use of a perimeter firewall that protects all of an organization's computers and a second internal firewall that protects a LAN.

A **packet-filtering firewall** examines each part of a message and determines whether to let that part pass. To make this decision, it examines the source address, the destination address(es), and other data.

Packet-filtering firewalls can prohibit outsiders from starting a session with any user behind the firewall. They can also disallow traffic from particular sites, such as known hacker addresses. They can prohibit traffic from legitimate, but unwanted, addresses, such as competitors' computers, and filter outbound traffic as well. They can keep employees from accessing specific sites, such as competitors' sites, sites with pornographic material, or popular news sites. As a future manager, if you have particular sites with which you do not want your employees to communicate, you can ask your IS department to enforce that limit via the firewalls.

**Figure 10-11**

Use of Multiple Firewalls

Packet-filtering firewalls are the simplest type of firewall. Other firewalls filter on a more sophisticated basis. If you take a data communications class, you will learn about them. For now, just understand that firewalls help to protect organizational computers from unauthorized network access.

No computer should connect to the Internet without firewall protection. Many ISPs provide firewalls for their customers. By nature, these firewalls are generic. Large organizations supplement such generic firewalls with their own. Most home routers include firewalls, and Microsoft Windows has a built-in firewall as well. Third parties also license firewall products.

## Malware Protection

The next technical safeguard in our list in Figure 10-9 concerns malware. **Malware** is a broad category of software that includes viruses, spyware, and adware.

- A **virus** is a computer program that replicates itself. Unchecked replication is like computer cancer; ultimately, the virus consumes the computer's resources. Furthermore, many viruses also take unwanted and harmful actions. The program code that causes the unwanted actions is called the payload. The **payload** can delete programs or data—or, even worse, modify data in undetected ways.
- **Trojan horses** are viruses that masquerade as useful programs or files. The name refers to the gigantic mock-up of a horse that was filled with soldiers and moved into Troy during the Trojan War. A typical Trojan horse appears to be a computer game, an MP3 music file, or some other useful, innocuous program.
- A **worm** is a virus that self-propagates using the Internet or other computer network. Worms spread faster than other virus types because they can replicate by themselves. Unlike nonworm viruses, which must wait for the user to share a file with a second computer, worms actively use the network to spread. Sometimes, worms can propagate so quickly that they overload and crash a network.
- **Spyware** programs are installed on the user's computer without the user's knowledge or permission. Spyware resides in the background and, unknown to the user, observes the user's actions and keystrokes, monitors computer activity, and reports the user's activities to sponsoring organizations. Some malicious spyware, called **key loggers**, captures keystrokes to obtain usernames, passwords, account numbers, and other sensitive information. Other spyware supports marketing analyses such as observing what users do, Web sites visited, products examined and purchased, and so forth.
- **Adware** is similar to spyware in that it is installed without the user's permission and resides in the background and observes user behavior. Most adware is benign in that it does not perform malicious acts or steal data. It does, however, watch user activity and produce pop-up ads. Adware can also change the user's default window or modify search results and switch the user's search engine.

Figure 10-12 lists some of the symptoms of adware and spyware. Sometimes these symptoms develop slowly over time as more malware components are installed. Should these symptoms occur on your computer, remove the spyware or adware using antimalware programs.

- Slow system startup
- Sluggish system performance
- Many pop-up advertisements
- Suspicious browser homepage changes
- Suspicious changes to the taskbar and other system interfaces
- Unusual hard-disk activity

**Figure 10-12**  
Spyware and Adware Symptoms

## Malware Safeguards

Fortunately, it is possible to avoid most malware using the following malware safeguards:

1. *Install antivirus and antispyware programs on your computer.* Your IS department will have a list of recommended (perhaps required) programs for this purpose. If you choose a program for yourself, choose one from a reputable vendor. Check reviews of antimalware software on the Web before purchasing.
2. *Set up your antimalware programs to scan your computer frequently.* You should scan your computer at least once a week and possibly more often. When you detect malware code, use the antimalware software to remove it. If the code cannot be removed, contact your IS department or antimalware vendor.
3. *Update malware definitions.* **Malware definitions**—patterns that exist in malware code—should be downloaded frequently. Antimalware vendors update these definitions continuously, and you should install these updates as they become available.
4. *Open email attachments only from known sources.* Also, even when opening attachments from known sources, do so with great care. With a properly configured firewall, email is the only outside-initiated traffic that can reach user computers.

Most antimalware programs check email attachments for malware code. However, all users should form the habit of *never* opening an email attachment from an unknown source. Also, if you receive an unexpected email from a known source or an email from a known source that has a suspicious subject, odd spelling, or poor grammar, do not open the attachment without first verifying with the known source that the attachment is legitimate.

5. *Promptly install software updates from legitimate sources.* Unfortunately, all programs are chock full of security holes; vendors are fixing them as rapidly as they are discovered, but the practice is inexact. Install patches to the operating system and application programs promptly.
6. *Browse only in reputable Internet neighborhoods.* It is possible for some malware to install itself when you do nothing more than open a Web page. Don't go there! Recently, malware writers have been paying for banner ads on legitimate sites that have malware embedded in the ad. One click and you're infected. Watch where you click.

## Design for Secure Applications

The final technical safeguard in Figure 10-9 concerns the design of applications. As you learned in the opening vignette, Michele and James are designing PRIDE with security in mind; PRIDE will store users' privacy settings in a database, and it will develop all applications to first read the privacy settings before revealing any data in exercise reports. Most likely, PRIDE will design its programs so that privacy data is processed by programs on servers; that design means that such data need be transmitted over the Internet only when it is created or modified.

By the way, a **SQL injection attack**, mentioned in the opening vignette and Chapter 5, occurs when users enter a SQL statement into a form in which they are supposed to enter a name or other data. If the program is improperly designed, it will accept this code and make it part of the database command that it issues. Improper data disclosure and data damage and loss are possible consequences. A well-designed application will make such injections ineffective.

As a future IS user, you will not design programs yourself. However, you should ensure that any information system developed for you and your department includes security as one of the application requirements.



## Q6 How Can Data Safeguards Protect Against Security Threats?

**Data safeguards** protect databases and other organizational data. Two organizational units are responsible for data safeguards. **Data administration** refers to an organization-wide function that is in charge of developing data policies and enforcing data standards.

**Database administration** refers to a function that pertains to a particular database. ERP, CRM, and MRP databases each have a database administration function. Database administration develops procedures and practices to ensure efficient and orderly multiuser processing of the database, to control changes to the database structure, and to protect the database. Database administration was summarized in Chapter 5.

Both data and database administration are involved in establishing the data safeguards in Figure 10-13. First, data administration should define data policies such as “We will not share identifying customer data with any other organization” and the like. Then data administration and database administration(s) work together to specify user data rights and responsibilities. Third, those rights should be enforced by user accounts that are authenticated at least by passwords.

The organization should protect sensitive data by storing it in encrypted form. Such encryption uses one or more keys in ways similar to that described for data communication encryption. One potential problem with stored data, however, is that the key might be lost or that disgruntled or terminated employees might destroy it. Because of this possibility, when data are encrypted, a trusted party should have a copy of the encryption key. This safety procedure is sometimes called **key escrow**.

Another data safeguard is to periodically create backup copies of database contents. The organization should store at least some of these backups off premises, possibly in a remote location. Additionally, IT personnel should periodically practice recovery to ensure that the backups are valid and that effective recovery procedures exist. Do not assume that just because a backup is made that the database is protected.

Physical security is another data safeguard. The computers that run the DBMS and all devices that store database data should reside in locked, controlled-access facilities. If not, they are subject not only to theft, but also to damage. For better security, the organization should keep a log showing who entered the facility, when, and for what purpose.

When organizations store databases in the cloud, all of the safeguards in Figure 10-13 should be part of the cloud service contract.

## Q7 How Can Human Safeguards Protect Against Security Threats?

**Human safeguards** involve the people and procedure components of information systems. In general, human safeguards result when authorized users follow appropriate procedures for system use and recovery. Restricting access to authorized users requires effective authentication

- Define data policies
- Data rights and responsibilities
- Rights enforced by user accounts authenticated by passwords
- Data encryption
- Backup and recovery procedures
- Physical security

**Figure 10-13**  
Data Safeguards

Read more about how to secure the security system in the Security Guide on pages 418–419.

methods and careful user account management. In addition, appropriate security procedures must be designed as part of every information system, and users should be trained on the importance and use of those procedures. In this section, we will consider the development of human safeguards for employees. According to the survey of computer crime discussed in Q2, crime from malicious insiders is increasing in frequency and cost. This fact makes safeguards even more important.

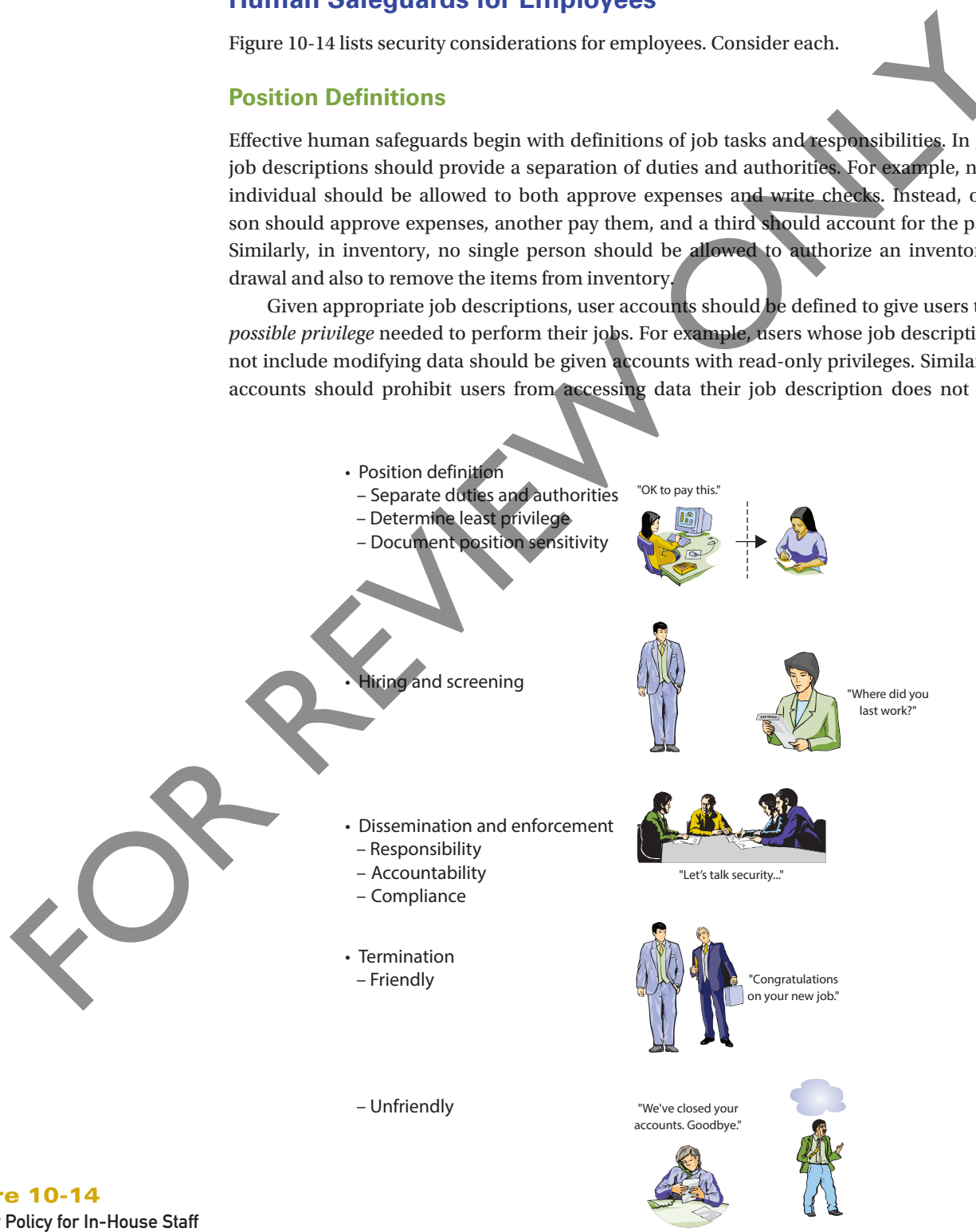
### Human Safeguards for Employees

Figure 10-14 lists security considerations for employees. Consider each.

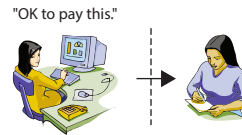
#### Position Definitions

Effective human safeguards begin with definitions of job tasks and responsibilities. In general, job descriptions should provide a separation of duties and authorities. For example, no single individual should be allowed to both approve expenses and write checks. Instead, one person should approve expenses, another pay them, and a third should account for the payment. Similarly, in inventory, no single person should be allowed to authorize an inventory withdrawal and also to remove the items from inventory.

Given appropriate job descriptions, user accounts should be defined to give users the *least possible privilege* needed to perform their jobs. For example, users whose job description does not include modifying data should be given accounts with read-only privileges. Similarly, user accounts should prohibit users from accessing data their job description does not require.



- Position definition
  - Separate duties and authorities
  - Determine least privilege
  - Document position sensitivity



- Hiring and screening



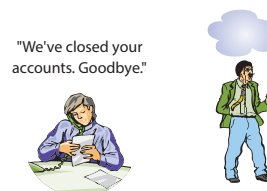
- Dissemination and enforcement
  - Responsibility
  - Accountability
  - Compliance



- Termination
  - Friendly



- Unfriendly



**Figure 10-14**  
Security Policy for In-House Staff

Because of the problem of semantic security, even access to seemingly innocuous data may need to be limited.

Finally, the security sensitivity should be documented for each position. Some jobs involve highly sensitive data (e.g., employee compensation, salesperson quotas, and proprietary marketing or technical data). Other positions involve no sensitive data. Documenting *position sensitivity* enables security personnel to prioritize their activities in accordance with the possible risk and loss.

### Hiring and Screening

Security considerations should be part of the hiring process. Of course, if the position involves no sensitive data and no access to information systems, then screening for information systems security purposes will be minimal. When hiring for high-sensitivity positions, however, extensive interviews, references, and background investigations are appropriate. Note, too, that security screening applies not only to new employees, but also to employees who are promoted into sensitive positions.

### Dissemination and Enforcement

Employees cannot be expected to follow security policies and procedures that they do not know about. Therefore, employees need to be made aware of the security policies, procedures, and responsibilities they will have.

Employee security training begins during new-employee training, with the explanation of general security policies and procedures. That general training must be amplified in accordance with the position's sensitivity and responsibilities. Promoted employees should receive security training that is appropriate to their new positions. The company should not provide user accounts and passwords until employees have completed required security training.

Enforcement consists of three interdependent factors: responsibility, accountability, and compliance. First, the company should clearly define the security *responsibilities* of each position. The design of the security program should be such that employees can be held *accountable* for security violations. Procedures should exist so that when critical data are lost, it is possible to determine how the loss occurred and who is accountable. Finally, the security program should encourage security *compliance*. Employee activities should regularly be monitored for compliance, and management should specify the disciplinary action to be taken in light of noncompliance.

Management attitude is crucial: Employee compliance is greater when management demonstrates, both in word and deed, a serious concern for security. If managers write passwords on staff bulletin boards, shout passwords down hallways, or ignore physical security procedures, then employee security attitudes and employee security compliance will suffer. Note, too, that effective security is a continuing management responsibility. Regular reminders about security are essential.

### Termination

Companies also must establish security policies and procedures for the termination of employees. Many employee terminations are friendly and occur as the result of promotion or retirement or when the employee resigns to take another position. Standard human resources policies should ensure that system administrators receive notification in advance of the employee's last day so that they can remove accounts and passwords. The need to recover keys for encrypted data and any other special security requirements should be part of the employee's out-processing.

Unfriendly termination is more difficult because employees may be tempted to take malicious or harmful actions. In such a case, system administrators may need to remove user accounts and passwords prior to notifying the employee of his or her termination. Other actions

may be needed to protect the company's data assets. A terminated sales employee, for example, may attempt to take the company's confidential customer and sales-prospect data for future use at another company. The terminating employer should take steps to protect those data prior to the termination.

The human resources department should be aware of the importance of giving IS administrators early notification of employee termination. No blanket policy exists; the information systems department must assess each case on an individual basis.

## Human Safeguards for Nonemployee Personnel

Business requirements may necessitate opening information systems to nonemployee personnel—temporary personnel, vendors, partner personnel (employees of business partners), and the public. Although temporary personnel can be screened, to reduce costs the screening will be abbreviated from that for employees. In most cases, companies cannot screen either vendor or partner personnel. Of course, public users cannot be screened at all. Similar limitations pertain to security training and compliance testing.

In the case of temporary, vendor, and partner personnel, the contracts that govern the activity should call for security measures appropriate to the sensitivity of the data and the IS resources involved. Companies should require vendors and partners to perform appropriate screening and security training. The contract also should mention specific security responsibilities that are particular to the work to be performed. Companies should provide accounts and passwords with the least privilege and remove those accounts as soon as possible.

The situation differs with public users of Web sites and other openly accessible information systems. It is exceedingly difficult and expensive to hold public users accountable for security violations. In general, the best safeguard from threats from public users is to *harden* the Web site or other facility against attack as much as possible. **Hardening** a site means to take extraordinary measures to reduce a system's vulnerability. Hardened sites use special versions of the operating system, and they lock down or eliminate operating systems features and functions that are not required by the application. Hardening is actually a technical safeguard, but we mention it here as the most important safeguard against public users.

Finally, note that the business relationship with the public, and with some partners, differs from that with temporary personnel and vendors. The public and some partners use the information system to receive a benefit. Consequently, safeguards need to protect such users from internal company security problems. A disgruntled employee who maliciously changes prices on a Web site potentially damages both public users and business partners. As one IT manager put it, "Rather than protecting ourselves from them, we need to protect them from us." This is an extension of the fifth guideline in Figure 10-8.

## Account Administration

The administration of user accounts, passwords, and help-desk policies and procedures is another important human safeguard.

### Account Management

Account management concerns the creation of new user accounts, the modification of existing account permissions, and the removal of unneeded accounts. Information system administrators perform all of these tasks, but account users have the responsibility to notify the administrators of the need for these actions. The IS department should create standard procedures for this purpose. As a future user, you can improve your relationship with IS personnel by providing early and timely notification of the need for account changes.

The existence of accounts that are no longer necessary is a serious security threat. IS administrators cannot know when an account should be removed; it is up to users and managers to give such notification.

### Figure 10-15 Sample Account Acknowledgment Form

Source: National Institute of Standards and Technology, Introduction to Computer Security: The NIST Handbook, Publication 800-812

I hereby acknowledge personal receipt of the system password(s) associated with the user IDs listed below. I understand that I am responsible for protecting the password(s), will comply with all applicable system security standards, and will not divulge my password(s) to any person. I further understand that I must report to the Information Systems Security Officer any problem I encounter in the use of the password(s) or when I have reason to believe that the private nature of my password(s) has been compromised.

## Password Management

Passwords are the primary means of authentication. They are important not just for access to the user's computer, but also for authentication to other networks and servers to which the user may have access. Because of the importance of passwords, the National Institute of Standards and Technology (NIST) recommends that employees be required to sign statements similar to those shown in Figure 10-15.

When an account is created, users should immediately change the password they are given to one of their own. In fact, well-constructed systems require the user to change the password on first use.

Additionally, users should change passwords frequently thereafter. Some systems will require a password change every 3 months or perhaps more frequently. Users grumble at the nuisance of making such changes, but frequent password changes reduce not only the risk of password loss, but also the extent of damage if an existing password is compromised.

Some users create two passwords and switch back and forth between those two. This strategy results in poor security, and some password systems do not allow the user to reuse recently used passwords. Again, users may view this policy as a nuisance, but it is important.

## Help-Desk Policies

In the past, help desks have been a serious security risk. A user who had forgotten his password would call the help desk and plead for the help-desk representative to tell him his password or to reset the password to something else. "I can't get this report out without it!" was (and is) a common lament.

The problem for help-desk representatives is, of course, that they have no way of determining that they are talking with the true user and not someone spoofing a true user. But they are in a bind: If they do not help in some way, the help desk is perceived to be the "unhelpful desk."

To resolve such problems, many systems give the help-desk representative a means of authenticating the user. Typically, the help-desk information system has answers to questions that only the true user would know, such as the user's birthplace, mother's maiden name, or last four digits of an important account number. Usually, when a password is changed, notification of that change is sent to the user in an email. Email is sent as plaintext, however, so the new password itself ought not to be emailed. If you ever receive notification that your password was reset when you did not request such a reset, immediately contact IT security. Someone has compromised your account.

All such help-desk measures reduce the strength of the security system, and, if the employee's position is sufficiently sensitive, they may create too large a vulnerability. In such a case, the user may just be out of luck. The account will be deleted, and the user must repeat the account-application process.

## Systems Procedures

Figure 10-16 shows a grid of procedure types—normal operation, backup, and recovery. Procedures of each type should exist for each information system. For example, the order-entry system will have procedures of each of these types, as will the Web storefront, the inventory



	System Users	Operations Personnel
<b>Normal operation</b>	Use the system to perform job tasks, with security appropriate to sensitivity.	Operate data center equipment, manage networks, run Web servers, and do related operational tasks.
<b>Backup</b>	Prepare for loss of system functionality.	Back up Web site resources, databases, administrative data, account and password data, and other data.
<b>Recovery</b>	Accomplish job tasks during failure. Know tasks to do during system recovery.	Recover systems from backed up data. Perform role of help desk during recovery.

**Figure 10-16**  
Systems Procedures

system, and so forth. The definition and use of standardized procedures reduces the likelihood of computer crime and other malicious activity by insiders. It also ensures that the system's security policy is enforced.

Procedures exist for both users and operations personnel. For each type of user, the company should develop procedures for normal, backup, and recovery operations. As a future user, you will be primarily concerned with user procedures. Normal-use procedures should provide safeguards appropriate to the sensitivity of the information system.

Backup procedures concern the creation of backup data to be used in the event of failure. Whereas operations personnel have the responsibility for backing up system databases and other systems data, departmental personnel have the need to back up data on their own computers. Good questions to ponder are, "What would happen if I lost my computer or mobile device tomorrow?" "What would happen if someone dropped my computer during an airport security inspection?" "What would happen if my computer was stolen?" Employees should ensure that they back up critical business data on their computers. The IS department may help in this effort by designing backup procedures and making backup facilities available.

Finally, systems analysts should develop procedures for system recovery. First, how will the department manage its affairs when a critical system is unavailable? Customers will want to order and manufacturing will want to remove items from inventory even though a critical information system is unavailable. How will the department respond? Once the system is returned to service, how will records of business activities during the outage be entered into the system? How will service be resumed? The system developers should ask and answer these questions and others like them and develop procedures accordingly.

## Security Monitoring

Security monitoring is the last of the human safeguards we will consider. Important monitoring functions are activity log analyses, security testing, and investigating and learning from security incidents.

Many information system programs produce *activity logs*. Firewalls produce logs of their activities, including lists of all dropped packets, infiltration attempts, and unauthorized access attempts from within the firewall. DBMS products produce logs of successful and failed log-ins. Web servers produce voluminous logs of Web activities. The operating systems in personal computers can produce logs of log-ins and firewall activities.

None of these logs adds any value to an organization unless someone looks at them. Accordingly, an important security function is to analyze these logs for threat patterns, successful and unsuccessful attacks, and evidence of security vulnerabilities.

Today, most large organizations actively investigate their security vulnerabilities. They may employ utilities such as Tenable's Nessus or IBM's Security AppScan to assess their vulnerabilities.

Many companies create **honeypots**, which are false targets for computer criminals to attack. To an intruder, a honeypot looks like a particularly valuable resource, such as an unprotected Web site, but in actuality the only site content is a program that determines the attacker's IP address. Organizations can then trace the IP address back using free online tools, like DNSstuff, to determine who has attacked them.<sup>12</sup> If you are technically minded, detail-oriented, and curious, a career as a security specialist in this field is almost as exciting as it appears on *CSI*. To learn more, check out DNSstuff, Nessus, or Security AppScan. See also *Applied Information Security*, 2nd ed.<sup>13</sup>

Another important monitoring function is to investigate security incidents. How did the problem occur? Have safeguards been created to prevent a recurrence of such problems? Does the incident indicate vulnerabilities in other portions of the security system? What else can be learned from the incident?

Security systems reside in a dynamic environment. Organization structures change. Companies are acquired or sold; mergers occur. New systems require new security measures. New technology changes the security landscape, and new threats arise. Security personnel must constantly monitor the situation and determine if the existing security policy and safeguards are adequate. If changes are needed, security personnel need to take appropriate action.

Security, like quality, is an ongoing process. There is no final state that represents a secure system or company. Instead, companies must monitor security on a continuing basis.

## Q8 How Should Organizations Respond to Security Incidents?

The last component of a security plan that we will consider is incident response. Figure 10-17 lists the major factors. First, every organization should have an incident-response plan as part of the security program. No organization should wait until some asset has been lost or compromised before deciding what to do. The plan should include how employees are to respond to security problems, whom they should contact, the reports they should make, and steps they can take to reduce further loss.

Consider, for example, a virus. An incident-response plan will stipulate what an employee should do when he notices the virus. It should specify whom to contact and what to do. It may stipulate that the employee should turn off his computer and physically disconnect from the network. The plan should also indicate what users with wireless computers should do.

The plan should provide centralized reporting of all security incidents. Such reporting will enable an organization to determine if it is under systematic attack or whether an incident is isolated. Centralized reporting also allows the organization to learn about security threats, take consistent actions in response, and apply specialized expertise to all security problems.

- Have plan in place
- Centralized reporting
- Specific responses
  - Speed
  - Preparation pays
  - Don't make problem worse
- Practice

**Figure 10-17**  
Factors in Incident Response

<sup>12</sup>For this reason, do *not* attempt to scan servers for fun. It won't take the organization very long to find you, and it will not be amused!

<sup>13</sup>Randall Boyle and Jeffrey Proudfoot, *Applied Information Security*, 2nd ed. (Upper Saddle River, NJ: Pearson Education, 2014).

When an incident does occur, speed is of the essence. The longer the incident goes on, the greater the cost. Viruses and worms can spread very quickly across an organization's networks, and a fast response will help to mitigate the consequences. Because of the need for speed, preparation pays. The incident-response plan should identify critical personnel and their off-hours contact information. These personnel should be trained on where to go and what to do when they get there. Without adequate preparation, there is substantial risk that the actions of well-meaning people will make the problem worse. Also, the rumor mill will be alive with all sorts of nutty ideas about what to do. A cadre of well-informed, trained personnel will serve to dampen such rumors.

Finally, organizations should periodically practice incident response. Without such practice, personnel will be poorly informed on the response plan, and the plan itself may have flaws that only become apparent during a drill.

Q9

2025?



What will be the status of information security by 2025? Will we have found a magic bullet to eliminate security problems? No. Human error is a constant; well-managed organizations will plan better for it and know how to respond better when it does occur, but as long as we have humans, we'll have error. Natural disasters are similar. The horrific events surrounding Hurricane Katrina in 2005 and the Japanese tsunami in 2011, as well as Hurricane Sandy in 2012, have alerted the world that we need to be better prepared, and more companies will set up hot or cold sites and put more data in well-prepared clouds. So, we'll be better prepared, but natural disasters are natural, after all.

Unfortunately, it is likely that sometime in the next 10 years some new, major incidents of cyberwarfare will have occurred. APTs will become more common, if indeed, they are not already common but we don't know it. It would appear that both Stuxnet and Flame have been in operation for 4 or 5 years. Will those who were damaged by them retaliate? It seems likely they will, at least, try. Will some new nation or group enter the cyberwar picture? That also seems likely. Unless you're in the security and intelligence business, there isn't much you can do about it. But don't be surprised if some serious damage is inflicted somewhere in the world due to APTs.

As of June 2014, many U.S. citizens are concerned with PRISM, the intelligence program by which the National Security Agency (NSA) requested and received data about Internet activities from major Internet providers. After the initial hullabaloo, it appears that Internet providers did not allow the government direct access to their servers, but rather delivered only data about specific individuals, as legally requested according to security laws enacted after 9/11. If so, then PRISM represents a legal governmental request for data, different only in scale from a governmental request for banking data about an organized crime figure. As of June 2014, Edward Snowden, the man who exposed the PRISM program, appears to be either an advocate for Internet freedom and privacy or a traitor who sold government secrets to China and Russia for private gain. Regardless of the reasons for the leak, the episode does raise the question of what governmental intrusion should be allowed into private data. We can hope the revelation of the existence of PRISM will spark a public conversation on the balance of national security and data privacy.

What about computer crime? It is a game of cat and mouse. Computer criminals find a vulnerability to exploit, and they exploit it. Computer security experts discover that vulnerability and create safeguards to thwart it. Computer criminals find a new vulnerability to exploit, computer security forces thwart it, and so it goes. The next major challenges will likely be those

affecting mobile devices. But security on these devices will be improved as threats emerge that exploit their vulnerabilities. This cat-and-mouse game is likely to continue for at least the next 10 years. No super-safeguard will be devised to prevent computer crime, nor will any particular computer crime be impossible to thwart. However, the skill level of this cat-and-mouse activity is likely to increase, and substantially so. Because of increased security in operating systems and other software, and because of improved security procedures and employee training, it will become harder and harder for the lone hacker to find some vulnerability to exploit. Not impossible, but vastly more difficult.

So, what will happen? Cloud vendors and major organizations will continue to invest in safeguards; they'll hire more people (maybe you), train them well, and become ever more difficult to infiltrate. Although some criminals will continue to attack these fortresses, most will turn their attention to less protected, more vulnerable, midsized and smaller organizations and to individuals. You can steal \$50 million from one company or \$50 from a million people with the same cash result. And, in the next 10 years, because of improved security at large organizations, the difficulty and cost of stealing that \$50 million will be much higher than stealing \$50 a million times. Take another look at Figure 10-7—and not for the purpose of the exam!

Part of the problem is porous national borders. People can freely enter the United States electronically without a passport. They can commit crimes with little fear of repercussions. There are no real electronic IDs. Cyber-gangs are well organized, financially motivated, and possibly state-sponsored. Electronic lawlessness is the order of the day. If someone in Romania steals from Google, Apple, Microsoft, or Boeing and then disappears into a cloud of networks in Uzbekistan, do those large organizations have the resources, expertise, and legal authority to pursue the attackers? What if that same criminal steals from you in Nashville? Can your local or state law enforcement authorities help? And, if your portion of the crime is for \$50, how many calls to Uzbekistan do they want to make?

At the federal level, finances and politics take precedence over electronic security. The situation will likely be solved as it was in the past. Strong local “electronic” sheriffs will take control of their electronic borders and enforce existing laws. It will take at least a couple decades for this to happen. Technology is moving faster than either the public or elected officials can educate themselves.

Take yet another look at Figure 10-7. Send a copy to your loved ones.

# Security Guide

## A LOOK THROUGH NSA'S PRISM

**As stated in Q1**, security is a trade-off. You can get better security, but you have to give up some freedom. The more secure you want to be, the more freedom you have to give up. It's a simple relationship to understand, but hard to recognize in your life.

Take car insurance as an example. It gives you the security of knowing you'll be protected against financial hardship if you're in an accident. But the trade-off is that you have to give up the freedom to spend your insurance premiums on something else. You get security, but it costs you.

An organizational security policy requiring users to use strong passwords works the same way. The organization gets the security of knowing its passwords will be hard to crack if stolen, thus protecting its information systems. However, users lose the freedom of choosing any password they like. The organization may also experience other losses in the form of reduced employee productivity or lower morale.

It's important to understand the trade-off between security and freedom because you'll hear people talk about getting more of one without talking about losing the other. A prominent example of this is the recent revelation of the National Security Agency's (NSA) PRISM program.

### NSA's PRISM

On June 6, 2013, Edward Snowden leaked top-secret PowerPoint slides detailing the NSA's secret global surveillance program codenamed **PRISM**. The PRISM program started in 2007 and was designed to access data from nine service providers: Google, Microsoft, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, and Apple.<sup>14</sup>

PRISM, according to the leaked slides, was designed to access email, videos, photos, video and voice chat, file transfers,

VoIP, stored data, videoconferencing, login activity, social networking activity, and something called "special requests" at service providers. Google, Microsoft, Yahoo!, and Facebook categorically denied providing access to the U.S. government except for a relatively small number of specific requests.<sup>15</sup>

The public doesn't know how many people have been affected by PRISM, but a 2014 transparency report put out by the Office of the Director of Intelligence indicated that 89,138 "targets" were spied on during 2013. The only problem is that a "target" could refer to individuals, groups, companies, foreign powers, or even a facility. It's likely the actual number of people affected could be several orders of magnitude larger.<sup>16</sup>

### The Privacy Versus Security Trade-off

Privacy advocates were outraged at the existence of PRISM and called for congressional investigations. They claimed that their **privacy**, or freedom from being observed by other people, was being destroyed in the name of **security**, or state of being free from danger. The Internet companies involved faced



<sup>14</sup>Timothy Lee, "Here's Everything We Know About PRISM to Date," *The Washington Post*, June 12, 2013, accessed June 27, 2014, [www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/](http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/).

<sup>15</sup>Ibid.

<sup>16</sup>Kim Zetter, "U.S. Says It Spied on 89,000 Targets Last Year, but the Number Is Deceptive," *Wired*, June 27, 2014, [www.wired.com/2014/06/90000-foreigners-targeted-for-spying/](http://www.wired.com/2014/06/90000-foreigners-targeted-for-spying/).



substantial backlash from customers claiming they were aiding the U.S. government in their efforts to erode their civil liberties.

Edward Snowden commented on PRISM, saying, “If we want to be free, we can’t become subject to surveillance. We can’t give away our privacy.”<sup>17</sup> James R. Clapper, director of National Intelligence, stated “the unauthorized disclosure of information about this important and entirely legal program is reprehensible and risks important protections for the security of Americans.”<sup>18</sup> White House Spokesman Josh Earnest summed it up by saying, “The President welcomes a discussion of the trade-offs between security and civil liberties.”<sup>19</sup>

For centuries people have known that security comes at a cost. Jean Jacques Rousseau’s 1762 book *The Social Contract or Principles of Political Right* quotes Count Palatine of Posen in Latin: “*Malo periculosam, libertatem quam quietam servitutem*,” which translates as “I prefer dangerous freedom over peaceful slavery.”

So, the important question becomes, when you look through NSA’s PRISM do you see it providing increased security or reducing your freedom from being observed, in other words, your privacy? Put another way, are you concerned about being more secure or having more freedom in your life? Undoubtedly your values, beliefs, and past experiences color your answers to these questions.

Another way to think about this trade-off is to imagine how your behavior might change if you were constantly being monitored. Would you still get those

delicious-tasting hamburgers at the seedy bar down the street or stop going there because you’re worried credit card charges could be used against you somehow? Would you still hang out with friends from other countries or stop because you’re worried it might somehow prevent you from getting a security clearance? Would you have behaved differently on your date last week if a parent was silently taking notes in the back seat?

## The Trade-off in Organizations

Understanding the trade-off between security and freedom will help you see the rationale behind organizational security policies and procedures. You’ll understand that someone touting improved security is also indirectly advocating a loss of freedom in some manner. The contrary is also true.

For example, some people find the PRISM monitoring to be too invasive. They want to live their lives without their government spying on them. But monitoring does have its benefits. It could be used to make you safer by stopping a terrorist attack. Similarly, employee monitoring can be seen as too invasive. But it can also be used to reduce theft. In the end, it’s a balancing act.

Can you have both great security and lots of freedom? Information security managers try to do just that. They try to prevent losses like data theft (security) while enabling innovation (freedom). In short, they try to be like bulletproof glass—protective and transparent.



## DISCUSSION QUESTIONS

1. Using both the categorical imperative (pages 20–21) and utilitarianism (pages 56–57), assess the ethics of spying. Consider a government spying on its own citizens, foreign militaries, foreign governments, foreign corporations, or foreign citizens.
2. Describe what you think should be done with the NSA’s PRISM program. Should it be continued without change, given more public oversight, substantially reduced in functionality, or discontinued altogether? Justify your decision.
3. Without the illegal disclosure of top-secret documents by Edward Snowden, the PRISM program may never have been discovered. Were Snowden’s actions ethical? Consider both the categorical imperative and utilitarianism perspectives in your response.
4. What is your opinion of employee monitoring? What effect does employee monitoring have on employee morale? How could employee monitoring make the organization more secure?
5. Describe the differences between freedom and privacy. Does a loss of privacy always mean a loss of freedom? If so, freedom from what? Can you lose freedom without losing privacy? Describe how your conclusions about the differences in these words pertain to PRISM.

<sup>17</sup>Matthew Cole, Richard Esposito, Bill Dedman, and Mark Schone, “Traitor or Patriot? Edward Snowden Sits Down with Brian Williams,” NBC News, May 28, 2014, [www.nbcnews.com/feature/edward-snowden-interview/traitor-or-patriot-edward-snowden-sits-down-brian-williams-n117006](http://www.nbcnews.com/feature/edward-snowden-interview/traitor-or-patriot-edward-snowden-sits-down-brian-williams-n117006).

<sup>18</sup>Charlie Savage, Edward Wyatt, Peter Baker, and Michael Shear, “Intelligence Chief Calls Leaks on U.S. Data Collection ‘Reprehensible,’” *The New York Times*, June 7, 2013, accessed June 28, 2014, [www.nytimes.com/2013/06/08/us/intelligence-chief-calls-leaks-on-us-data-collection-reprehensible.html](http://www.nytimes.com/2013/06/08/us/intelligence-chief-calls-leaks-on-us-data-collection-reprehensible.html).

<sup>19</sup>Ibid.

# Guide

## PHISHING FOR CREDIT CARDS, IDENTIFYING NUMBERS, BANK ACCOUNTS

A **phisher** is an individual or organization that spoofs legitimate companies in an attempt to illegally capture personal data such as credit card numbers, email accounts, and driver's license numbers. Some phishers install malicious program code on users' computers as well.

Phishing is usually initiated via email. Phishers steal legitimate logos and trademarks and use official-sounding words in an attempt to fool users into revealing personal data or clicking a link. Phishers do not bother with laws about trademark use. They place names and logos like Visa, MasterCard, Discover, and American Express on their Web pages and use them as bait. In some cases,

phishers copy the entire look and feel of a legitimate company's Web site.

In this exercise, you and a group of your fellow students will be asked to investigate phishing attacks. If you search the Web for *phishing*, be aware that your search may bring the attention of an active phisher. Therefore, do not give any data to any site that you visit as part of this exercise!



Source: Carlos\_bcn/Fotolia

Your Order ID: "17152492"  
Order Date: "09/07/12"  
Product Purchased: "Two First Class Tickets to Cozumel"  
Your card type: "CREDIT"  
Total Price: "\$349.00"

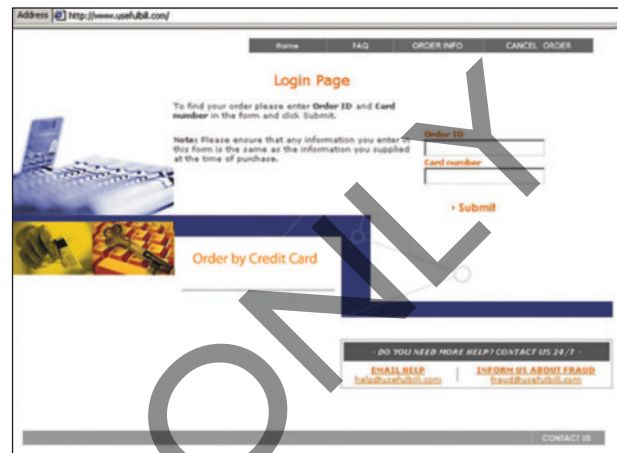
Hello, when you purchased your tickets you provided an incorrect mailing address.

[See more details here](#)

Please follow the link and modify your mailing address or cancel your order. If you have questions, feel free to contact us [account@usefulbill.com](mailto:account@usefulbill.com)

**Figure 1**

Fake Phishing Email



**Figure 2**

Fake Phishing Screen



## DISCUSSION QUESTIONS

- To learn the fundamentals of phishing, visit the following site: [www.microsoft.com/protect/fraud/phishing/symptoms.aspx](http://www.microsoft.com/protect/fraud/phishing/symptoms.aspx). To see recent examples of phishing attacks, visit [www.fraudwatchinternational.com/phishing/](http://www.fraudwatchinternational.com/phishing/).
  - Using examples from these Web sites, describe how phishing works.
  - Explain why a link that appears to be legitimate, such as [www.microsoft.mysite.com](http://www.microsoft.mysite.com) may, in fact, be a link to a phisher's site.
  - List five indicators of a phishing attack.
  - Write an email that you could send to a friend or relative who is not well versed in technical matters that explains what phishing is and how that person can avoid it.
- Suppose you received the email in Figure 1 and mistakenly clicked *See more details here*. When you did so, you were taken to the Web page shown in Figure 2. List every phishing symptom that you find in these two figures and explain why it is a symptom.
- Suppose you work for an organization that is being phished.
  - How would you learn that your organization is being attacked?
  - What steps should your organization take in response to the attack?
  - What liability, if any, do you think your organization has for damages to customers that result from a phishing attack that carries your brand and trademarks?
- Summarize why phishing is a serious problem to commerce today.
- Describe actions that industry organizations, companies, governments, or individuals can take to help reduce phishing.



## ACTIVE REVIEW

Use this Active Review to verify that you understand the ideas and concepts that answer the chapter's study questions.

### Q1 What is the goal of information systems security?

Define *threat*, *vulnerability*, *safeguard*, and *target*. Give an example of each. List three types of threats and five types of security losses. Give different examples for the three rows of Figure 10-2. Summarize each of the elements in the cells of Figure 10-3. Explain why it is difficult to know the true cost of computer crime. Explain the goal of IS security.

### Q2 How big is the computer security problem?

Explain why it is difficult to know the true size of the computer security problem in general and of computer crime in particular. List the takeaways in this question and explain the meaning of each.

### Q3 How should you respond to security threats?

Explain each of the elements in Figure 10-7. Define *IDS*, and explain why the use of an IDS program is sobering, to say the least. Define *brute force attack*. Summarize the characteristics of a strong password. Explain how your identity and password do more than just open doors on your computer. Define *cookie* and explain why using a program like CCleaner is a good example of the computer security trade-off.

### Q4 How should organizations respond to security threats?

Name and describe two security functions that senior management should address. Summarize the contents of a security policy. Explain what it means to manage risk. Summarize the steps that organizations should take when balancing risk and cost.

### Q5 How can technical safeguards protect against security threats?

List five technical safeguards. Define *identification* and *authentication*. Describe three types of authentication. Explain how SSL/TLS works. Define *firewall*, and explain its purpose.

Define *malware*, and name five types of malware. Describe six ways to protect against malware. Summarize why malware is a serious problem. Explain how PRIDE is designed for security.

### Q6 How can data safeguards protect against security threats?

Define *data administration* and *database administration*, and explain their difference. List data safeguards.

### Q7 How can human safeguards protect against security threats?

Summarize human safeguards for each activity in Figure 10-13. Summarize safeguards that pertain to nonemployee personnel. Describe three dimensions of safeguards for account administration. Explain how system procedures can serve as human safeguards. Describe security monitoring techniques.

### Q8 How should organizations respond to security incidents?

Summarize the actions that an organization should take when dealing with a security incident.

### Q9 2025?

What, in the opinion of the author, is likely to happen regarding cyberwarfare in the next 10 years? Explain how the phrase *cat and mouse* pertains to the evolution of computer crime. Describe the types of security problems that are likely to occur in the next 10 years. Explain how the focus of computer criminals will likely change in the next 10 years. Explain how this is likely to impact smaller organizations, and you.


## Using Your Knowledge with PRIDE

As an employee, investor, or advisor to PRIDE Systems, you can use the knowledge of this chapter to understand the security threats to which any business is subject. You know the need to trade off cost versus risk. You also know three categories of safeguards and the major types of safeguards for each. And, Zev Friedman you know what it means to design for security. You can also help ensure that PRIDE Systems employees and PRIDE users create and use strong passwords.

## KEY TERMS AND CONCEPTS

Advanced Persistent Threat (APT) 394	https 405	Privacy Act of 1974 402
Adware 407	Human safeguards 409	Public key encryption 405
Asymmetric encryption 405	Identification 401	Safeguard 390
Authentication 401	Internal firewalls 406	Secure Sockets Layer (SSL) 405
Biometric authentication 404	Intrusion detection system (IDS) 397	Security 418
Brute force attack 397	IP spoofing 393	Smart cards 404
Cookies 398	Key 404	Sniffing 393
Data administration 409	Key escrow 409	Spoofing 393
Data safeguards 409	Key loggers 407	Spyware 407
Database administration 409	Malware 407	SQL injection attack 408
Denial of service (DoS) 394	Malware definitions 408	Symmetric encryption 405
Email spoofing 393	Packet-filtering firewall 406	Target 390
Encryption 404	Payload 407	Technical safeguards 401
Encryption algorithms 404	Perimeter firewall 406	Threat 390
Firewall 406	Personal identification number (PIN) 404	Transport Layer Security (TLS) 405
Gramm-Leach-Bliley (GLB) Act 402	Phisher 393	Trojan horses 407
Hacking 393	Phishing 393	Usurpation 393
Hardening 412	Pretexting 392	Virus 407
Health Insurance Portability and Accountability Act (HIPAA) 402	PRISM 418	Vulnerability 390
Honeypots 415	Privacy 418	Wardrivers 393
		Worm 407

**MyMISLab™**

Go to [mymislab.com](http://mymislab.com) to complete the problems marked with this icon .

## USING YOUR KNOWLEDGE

- ★ **10-1.** Credit reporting agencies are required to provide you with a free credit report each year. Most such reports do not include your credit score, but they do provide the details on which your credit score is based. Use one of the following companies to obtain your free report: *www.equifax.com*, *www.experion.com*, and *www.transunion.com*.
- You should review your credit report for obvious errors. However, other checks are appropriate. Search the Web for guidance on how best to review your credit records. Summarize what you learn.
  - What actions can you take if you find errors in your credit report?
  - Define *identity theft*. Search the Web and determine the best course of action if someone thinks he or she has been the victim of identity theft.
- ★ **10-2.** Suppose you lose your company laptop at an airport. What should you do? Does it matter what data are stored on your disk drive? If the computer contained sensitive or proprietary data, are you necessarily in trouble? Under what circumstances should you now focus on updating your resume for your new employer?
- ★ **10-3.** Suppose you alert your boss to the security threats in Figure 10-3 and to the safeguards in Figure 10-8. Suppose he says, “Very interesting. Tell me more.” In preparing for the meeting, you decide to create a list of talking points.
- Write a brief explanation of each threat in Figure 10-3.
  - Explain how the five components relate to safeguards.
  - Describe two to three technical, two to three data, and two to three human safeguards.
  - Write a brief description about the safeguards in Figure 10-13.
  - List security procedures that pertain to you, a temporary employee.
  - List procedures that your department should have with regard to disaster planning.



## COLLABORATION EXERCISE 10

Using the collaboration IS you built in Chapter 2 (page 74), collaborate with a group of students to answer the following questions.

The purpose of this activity is to assess the current state of computer crime.

**10-4.** Search the Web for the term *computer crime* and any related terms. Identify what you and your teammates think are the five most serious recent examples. Consider no crime that occurred more than 6 months ago. For each crime, summarize the loss that occurred and the circumstances surrounding the loss, and identify safeguards that were not in place or were ineffective in preventing the crime.

**10-5.** Search the Web for the term *computer crime statistics* and find two sources other than the Ponemon surveys cited in Q2.

- For each source, explain the methodology used and explain strengths and weaknesses of that methodology.
- Compare the data in the two new sources to that in Q2 and describe differences.
- Using your knowledge and intuition, describe why you think those differences occurred.

**10-6.** Go to <http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis> and download the 2013 report (or a more recent report if one is available).

- Summarize the survey with regard to safeguards and other measures that organizations use.
- Summarize the study's conclusions with regard to the efficacy of organizational security measures.
- Does your team agree with the conclusions in the study? Explain your answer.

**10-7.** Suppose that you are asked by your boss for a summary of what your organization should do with regard to computer security. Using the knowledge of this chapter and your answer to questions 10-4 - 10-6 above, create a PowerPoint presentation for your summary. Your presentation should include, but not be limited to:

- Definition of key terms
- Summary of threats
- Summary of safeguards
- Current trends in computer crime
- What senior managers should do about computer security
- What managers at all levels should do about computer security

## CASE STUDY 10

## Hitting the Target

On December 18, 2013, Target Corporation announced that it had lost 40 million credit and debit card numbers to attackers. Less than a month later Target announced an additional 70 million customer accounts were stolen that included names, emails, addresses, phone numbers, and so on.

After accounting for some overlap between the two data losses, it turns out that about 98 million customers were affected.<sup>20</sup> That's 31 percent of all 318 million people in the United States (including children and those without credit cards). This was one of the largest data breaches in U.S. history.

These records were stolen from point-of-sale (POS) systems at Target retail stores during the holiday shopping

season (November 27 to December 15, 2013). If you were shopping at a Target during this time, it's likely your data was lost. Below is a short summary of how attackers got away with that much data.

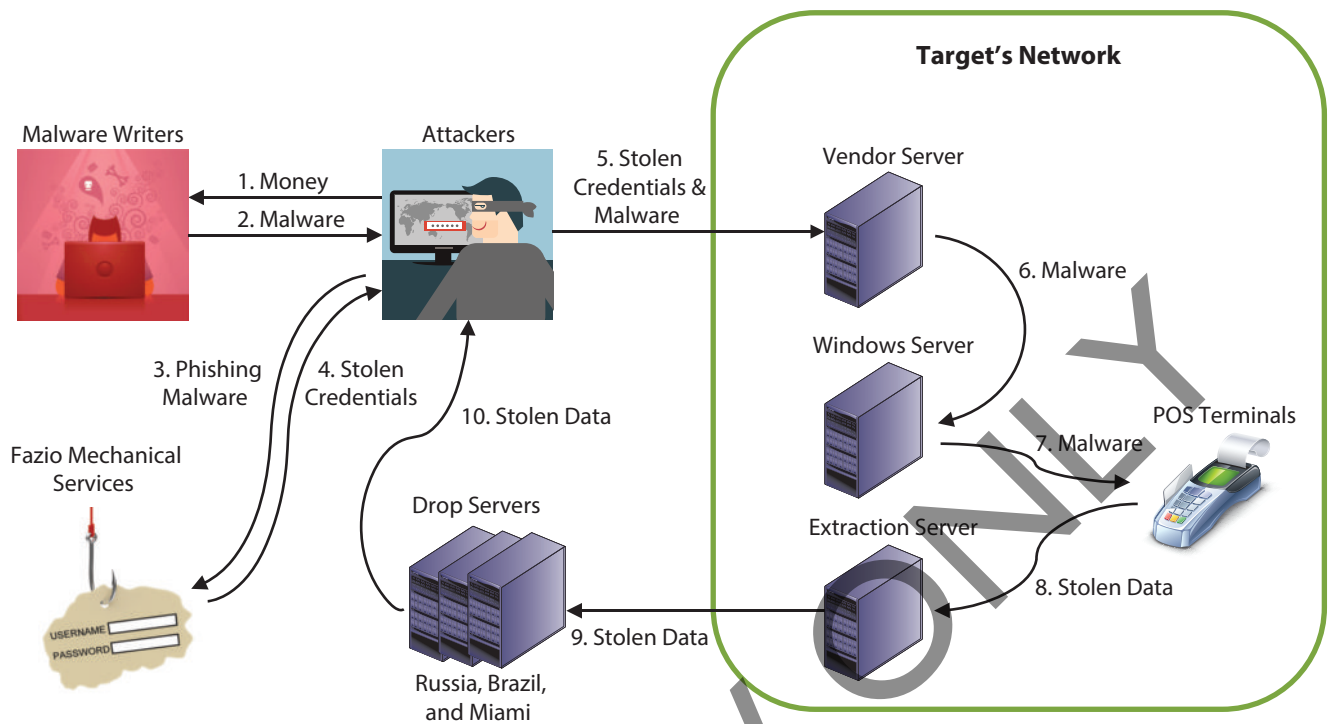
## How Did They Do It?

The attackers first used spear-phishing to infect a Target third-party vendor named Fazio Mechanical Services (refrigeration and HVAC services).<sup>21</sup> Attackers placed a piece of malware called Citadel to gather keystrokes, login credentials, and screenshots from Fazio users.<sup>22</sup> The attackers then used the stolen login credentials from Fazio to access a

<sup>20</sup>Ben Elgin, "Three New Details from Target's Credit Card Breach," *BusinessWeek*, March 26, 2014, accessed June 4, 2014, [www.businessweek.com/articles/2014-03-26/three-new-details-from-targets-credit-card-breach](http://www.businessweek.com/articles/2014-03-26/three-new-details-from-targets-credit-card-breach).

<sup>21</sup>Brian Krebs, "Target Hackers Broke In via HVAC Company," *KrebsOnSecurity.com*, February 5, 2014, accessed June 4, 2014, <http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company>.

<sup>22</sup>Chris Poulin, "What Retailers Need to Learn from the Target Data Breach to Protect Against Similar Attacks," *Security Intelligence*, January 31, 2014, accessed June 4, 2014, <http://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/#.U44ptPldUcS>.



**Figure 10-18**  
Target Data Breach

vendor portal (server) on Target's network. The attackers escalated privileges on that server and gained access to Target's internal network.

Once in, the attackers compromised an internal Windows file server. From this server the attackers used malware named Trojan.POSRAM (a variant of BlackPOS) to extract information from POS terminals. BlackPOS was developed by a 17-year-old from St. Petersburg, Russia, and can be purchased from underground sites for about \$2,000.<sup>23</sup>

The customer data was continuously sent from the POS terminals to an extraction server within Target's network. It was then funneled out of Target's network to drop servers in Russia, Brazil, and Miami. From there the data was taken and sold on the black market.

### The Damage

For the attackers, the "damage" was great. It's estimated that the attackers sold about 2 million credit cards for about \$26.85 each for a total profit of \$53.7 million.<sup>24</sup> Not bad for a few

weeks of work. Incentives for this type of criminal activity are substantial. Payoffs like these encourage even more data breaches.

Target, on the other hand, incurred much greater losses than the hacker's gains. Target will be forced to take a loss on all of the merchandise purchased using the stolen credit cards. It will also have to upgrade its payment terminals to support chip-and-PIN enabled cards (to prevent cloning cards from stolen information), pay increased insurance premiums, pay legal fees, settle with credit card processors, pay for consumer credit monitoring, and pay regulatory fines.

Target faces a loss of customer confidence and a drop in its revenues (a 46 percent loss for that quarter). Analysts put the direct loss to Target as high at \$450 million.<sup>25</sup> The company lost its CIO Beth Jacob and paid its CEO Gregg Steinhafel \$16 million to leave.<sup>26</sup>

The data breach affected more than just Target. Credit unions and banks will spend more than \$200 million issuing new cards.<sup>27</sup> Consumers will have to enroll in credit

<sup>23</sup>Swati Khandelwal, "BlackPOS Malware Used in Target Data Breach Developed by 17-Year-Old Russian Hacker," The Hacker News, January 17, 2014, accessed June 4, 2014, <http://thehackernews.com/2014/01/BlackPOS-Malware-russian-hacker-Target.html>.

<sup>24</sup>Brian Krebs, "The Target Breach, by the Numbers," *KrebsOnSecurity.com*, May 6, 2014, accessed June 4, 2014, <http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers>.

<sup>25</sup>Bruce Horowitz, "Data Breach Takes Toll on Target Profit," *USA Today*, February 26, 2014, accessed June 6, 2014, [www.usatoday.com/story/money/business/2014/02/26/target-earnings/5829469](http://www.usatoday.com/story/money/business/2014/02/26/target-earnings/5829469).

<sup>26</sup>Fred Donovan, "Target Breach: A Timeline," *FierceITSecurity.com*, February 18, 2014, accessed June 4, 2014, [www.fierceitsecurity.com/story/target-breach-timeline/2014-02-18](http://www.fierceitsecurity.com/story/target-breach-timeline/2014-02-18).

<sup>27</sup>Krebs, "The Target Breach, by the Numbers."

monitoring, continuously watch their credit, and fill out paperwork if fraudulent charges appear on their statements.

Insurance premiums for organizations other than Target will probably go up as well. Insurers may believe that more data breaches like this will occur in the future. Insurers will demand higher premiums, stricter controls, and more system auditing from organizations.

Just like car accidents, data breaches may not be viewed as important until *after* they occur. The data breach affected Target enough that it's upgrading its infrastructure, changing internal systems, and looking for a Chief Information Security Officer (CISO).<sup>28</sup>

Will there be a more severe data breach in the future? Probably. Are organizations ready for it? Based on past performance, we won't be ready for it until *after* it happens.

## QUESTIONS

- 10-8. Why did the attackers spear-phish a contractor to Target?
- 10-9. Explain how a third-party contractor could weaken an organization's overall security.
- 10-10. Describe how data was stolen from Target.
- 10-11. How might a data loss at one organization affect other organizations?
- 10-12. Explain why large organizations are attractive targets for attackers.
- 10-13. Why might chip-and-pin cards reduce this type of theft?
- 10-14. Why didn't Target have a CISO before the data breach?

### MyMISLab™

Go to [mymislab.com](http://mymislab.com) for Auto-graded writing questions as well as the following Assisted-graded writing questions:

- 10-15. Suppose you need to terminate an employee who works in your department. Summarize security protections you must take. How would you behave differently if this termination were a friendly one?
- 10-16. Read about MapReduce and Hadoop on pages 365–366 of Chapter 9 if you have not already done so. Is MapReduce suitable for password cracking? Explain your answer. Assume that it is. If it takes 4.5 years for one computer to crack a password, how long will it take 10,000 computers to crack one using Hadoop? If it takes 2 million years to crack a password, how long will it take 10,000 computers to crack one? What does this tell you about password construction?

<sup>28</sup>Dune Lawrence, "Target Taps an Outsider to Revamp IT Security After Massive Hack," *BusinessWeek*, April 29, 2014, accessed June 4, 2014, [www.businessweek.com/articles/2014-04-29/target-turns-to-an-outsider-for-cio-bob-derodes-to-revamp-it-security-after-massive-hack](http://www.businessweek.com/articles/2014-04-29/target-turns-to-an-outsider-for-cio-bob-derodes-to-revamp-it-security-after-massive-hack).