Chapter 13

Information Security: Barbarians at the Gateway (and Just About Everywhere Else)

13.1 Introduction

LEARNING OBJECTIVES

1. Recognize that information security breaches are on the rise.
2. Understand the potentially damaging impact of security breaches.
3. Recognize that information security must be made a top organizational priority.

Sitting in the parking lot of a Minneapolis Marshalls, a hacker armed with a laptop and a telescope-shaped antenna infiltrated the store's network via an insecure Wi-Fi base station.Particular thanks goes to my Boston College colleague, Professor Sam Ransbotham, whose advice, guidance, and suggestions were invaluable in creating this chapter. Any errors or omissions are entirely my own. The attack launched what would become a billion-dollar-plus nightmare scenario for TJX, the parent of retail chains that include Marshalls, Home Goods, and T. J. Maxx. Over a period of several months, the hacker and his gang stole at least 45.7 million credit and debit card numbers and pilfered driver's licenses and other private information from an additional 450,000 customers.E. Mills, "Attacks on Sony, Others, Show It's Open Hacking Season," *CNET*, June 8, 2011.

TJX, at the time a $17.5 billion *Fortune* 500 firm, was left reeling from the incident. The attack deeply damaged the firm's reputation. It burdened customers and banking partners with the time and cost of reissuing credit cards. And TJX suffered under settlement costs, payouts from court-imposed restitution, legal fees, and more. The firm estimated that it spent more than $150 million to correct security problems and settle with consumers affected by the breach, and that was just the tip of the iceberg. Estimates peg TJX's overall losses from this incident at between $1.35 billion and $4.5 billion.A. Matwyshyn, *Harboring Data: Information Security, Law, and the Corporation* (Palo Alto, CA: Stanford University Press, 2009).

A number of factors led to and amplified the severity of the TJX breach. There was a personnel betrayal: the mastermind was an alleged FBI informant who previously helped bring down a massive credit card theft scheme but then double-crossed the Feds and used insider information to help his gang outsmart the law and carry out subsequent hacks.D. Goldman, "Cybercrime: A Secret Underground Economy," *CNNMoney*, September 17, 2009. There was a technology lapse: TJX made itself an easy mark by using WEP, a wireless security technology less secure than the stuff many consumers use in their homes—one known for years to be trivially

compromised by the kind of "drive-by" hacking initiated by the perpetrators. And there was a procedural gaffe: retailers were in the process of rolling out a security rubric known as the Payment Card Industry Data Security Standard. Despite an industry deadline, however, TJX had requested and received an extension, delaying the rollout of mechanisms that might have discovered and plugged the hole before the hackers got in.K. Voigt, "Analysis: The Hidden Cost of Cybercrime," *CNN*, June 6, 2011.

The massive impact of the TJX breach should make it clear that security must be a top organizational priority. Attacks are on the rise. Security firm Symantec reported that in 2010, Web-based security attacks increased 93 percent over the prior year,*Synamtec Internet Security Threat Report*, Symantec Corporation, April 2011. and the first few months of 2011 saw shocking, high-profile attacks hit at several firms, including Sony, data provider Epsilon, Google, and even security software firm RSA.R. King, "Lessons from the Data Breach at Heartland," *BusinessWeek*, July 6, 2009. While the examples and scenarios presented here are shocking, the good news is that the vast majority of security breaches can be prevented. Let's be clear from the start: no text can provide an approach that will guarantee that you'll be 100 percent secure. And that's not the goal of this chapter. The issues raised in this brief introduction can, however, help make you aware of vulnerabilities; improve your critical thinking regarding current and future security issues; and help you consider whether a firm has technologies, training, policies, and procedures in place to assess risks, lessen the likelihood of damage, and respond in the event of a breach. A constant vigilance regarding security needs to be part of your individual skill set and a key component in your organization's culture. An awareness of the threats and approaches discussed in this chapter should help reduce your chance of becoming a victim.

As we examine security issues, we'll first need to understand what's happening, who's doing it, and what their motivation is. We'll then examine how these breaches are happening with a focus on technologies and procedures. Finally, we'll sum up with what can be done to minimize the risks of being victimized and quell potential damage of a breach for both the individual and the organization.

KEY TAKEAWAYS

- Information security is everyone's business and needs to be made a top organizational priority.
- Firms suffering a security breach can experience direct financial loss, exposed proprietary information, fines, legal payouts, court costs, damaged reputations, plummeting stock prices, and more.
- Information security isn't just a technology problem; a host of personnel and procedural factors can create and amplify a firm's vulnerability.

QUESTIONS AND EXERCISES

1. The 2011 data theft at database firm Epsilon impacted a number of the firm's clients, including Best Buy, Capital One, Citi, the Home Shopping Network, JP Morgan Chase, Kroger, Walgreens, and the College Board. Were you impacted by this breach (or any other)? How did you find out about the breach? Did you take action as a result? Research and report the estimated costs associated with this breach. Has the theft resulted in additional security issues for the individuals who had their data stolen?
2. As individuals or in groups assigned by your instructor, search online for recent reports on information security breaches. Come to class prepared to discuss the breach, its potential impact, and how it might have been avoided. What should the key takeaways be for managers studying your example?
3. Think of firms that you've done business with online. Search to see if these firms have experienced security breaches in the past. What have you found out? Does this change your attitude about dealing with the firm? Why or why not?
4. What factors were responsible for the TJX breach? Who was responsible for the breach? How do you think the firm should have responded?

13.2 Why Is This Happening? Who Is Doing It? And What's Their Motivation?

LEARNING OBJECTIVES

1. Understand the source and motivation of those initiating information security attacks.
2. Relate examples of various infiltrations in a way that helps raise organizational awareness of threats.

Thieves, vandals, and other bad guys have always existed, but the environment has changed. Today, nearly every organization is online, making any Internet-connected network a potential entry point for the growing worldwide community of computer criminals. Software and hardware solutions are also more complex than ever. Different vendors, each with their own potential weaknesses, provide technology components that may be compromised by misuse, misconfiguration, or mismanagement. Corporations have become data packrats, hoarding information in hopes of turning bits into bucks by licensing databases, targeting advertisements, or cross-selling products. And flatter organizations also mean that lower-level employees may be able to use technology to reach deep into corporate assets—amplifying threats from operator error, a renegade employee, or one compromised by external forces.

There are a lot of bad guys out there, and motivations vary widely, including the following:

- Account theft and illegal funds transfer
- Stealing personal or financial data
- Compromising computing assets for use in other crimes
- Extortion
- Espionage
- Cyberwarfare
- Terrorism
- Pranksters
- Protest hacking (hacktivism)
- Revenge (disgruntled employees)

Criminals stole more than $560 million from U.S. firms in 2009, and they did it "without drawing a gun or passing a note to a teller."S. Kroft, "Cyberwar: Sabotaging the System," *60 Minutes*, November 8, 2009; J. Leyden, "Cybercrime Losses Almost Double," *Register*, March 15, 2010. While some steal cash for their own use, others resell their hacking take to others. There is a thriving cybercrime underworld market in which **data harvesters**[1] sell to **cash-out fraudsters**[2]: criminals who might purchase data from the harvesters in order to buy (then resell) goods using stolen credit cards or create false accounts via identity theft. These collection and resale operations are efficient and sophisticated. Law enforcement has taken down sites like DarkMarket and ShadowCrew, in which card thieves and hacking tool peddlers received eBay-style seller ratings vouching for the "quality" of their wares.R. Singel, "Underground Crime Economy Health, Security Group Finds," *Wired*, November 24, 2008.

Hackers might also infiltrate computer systems to enlist hardware for subsequent illegal acts. A cybercrook might deliberately hop through several systems to make his path difficult to follow, slowing cross-border legal pursuit or even thwarting prosecution if launched from nations without extradition agreements.

In fact, your computer may be up for rent by cyber thieves right now. **Botnets**[3] of zombie computers (networks of infiltrated and compromised machines controlled by a central command) are used for all sorts of nefarious activity. This includes sending spam from thousands of difficult-to-shut-down accounts, launching tough-to-track click fraud efforts or staging what's known as **distributed denial of service (DDoS)**[4] attacks (effectively shutting down Web sites by overwhelming them with a crushing load of seemingly legitimate requests sent simultaneously by thousands of machines). Botnets have been discovered that are capable of sending out 100 billion spam messages a day,K. J. Higgins, "SecureWorks Unveils Research on Spamming Botnets," *DarkReading*, April 9, 2008. and botnets as large as 10 million zombies have been identified. Such systems theoretically control more computing power than the world's fastest supercomputers.B. Krebs, "Storm Worm Dwarfs World's Top Supercomputer," *Washington Post*, August 31, 2007.

Extortionists might leverage botnets or hacked data to demand payment to avoid retribution. Three eastern European gangsters used a botnet and threatened DDoS to extort $4 million from UK sports bookmakers,Trend Micro, "Web Threats Whitepaper," March 2008. while an extortion plot against the state of Virginia threatened to reveal names, Social Security numbers, and prescription information stolen from a medical records database.S. Kroft, "Cyberwar: Sabotaging the System," *60 Minutes*, November 8, 2009. Competition has also lowered the price to inflict such pain. *BusinessWeek* reports that the cost of renting out ten thousand machines, enough to cripple a site like Twitter, has tumbled to just $200 a day.J. Schectman, "Computer Hacking Made Easy," *BusinessWeek*, August 13, 2009.

1. Cybercriminals who infiltrate systems and collect data for illegal resale.
2. Firms that purchase assets from data harvesters. Actions may include using stolen credit card numbers to purchase goods, creating fake accounts via identity fraud, and more.
3. Hordes of surreptitiously infiltrated computers, linked and controlled remotely, also known as zombie networks
4. An attack where a firm's computer systems are flooded with thousands of seemingly legitimate requests, the sheer volume of which will slow or shut down the site's use. DDoS attacks are often performed via botnets.

Corporate espionage might be performed by insiders, rivals, or even foreign governments. Gary Min, a scientist working for DuPont, was busted when he tried to sell information valued at some $400 million, including R&D documents and secret data on proprietary products.J. Vijayan, "Software Consultant Who Stole Data on 110,000 People Gets Five-Year Sentence," *Computerworld*, July 10, 2007. Spies also breached the $300 billion U.S. Joint Strike Fighter project, siphoning off terabytes of data on navigation and other electronics systems.S. Gorman, A. Cole, and Y. Dreazen. "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, April 21, 2009. Hackers infiltrated security firm RSA, stealing data keys used in the firm's commercial authentication devices. The hackers then apparently leveraged the heist to enter the systems of RSA customers, U.S. Defense contractors L-3, Lockheed Martin, and Northrop Grumman.E. Mills, "China Linked to New Breaches Tied to RSA," *CNET*, June 6, 2011. Google has identified China as the nation of origin for a series of hacks targeting the Google accounts of diplomats and activists.P. Eckert, "Analysis: Can Naming, Shaming Curb Cyber Attacks from China?" *Reuters*, June 3, 2011. And the government of Tunisia even attempted a whole-scale hacking of local users' Facebook accounts during protests that eventually led to the ouster of the regime. The so-called man-in-the-middle style attack intercepted Facebook traffic at the state-affiliated ISP as it traveled between Tunisian Web surfers and Facebook's servers, enabling the government to steal passwords and delete posts and photos that criticized the regime.A. Madrigal, "The Inside Story of How Facebook Responded to Tunisian Hacks," *Atlantic*, January 24, 2011.

Cyberwarfare has also become a legitimate threat, with several attacks demonstrating how devastating technology disruptions by terrorists or a foreign power might be (see sidebar on Stuxnet). Brazil has seen hacks that cut off power to millions, and the *60 Minutes* news program showed a demonstration by "white hat" hackers that could compromise a key component in an oil refinery, force it to overheat, and cause an explosion. Taking out key components of the vulnerable U.S. power grid may be particularly devastating, as the equipment is expensive, much of it is no longer made in the United States, and some components may take three to four months to replace.S. Kroft, "Cyberwar: Sabotaging the System," *60 Minutes*, November 8, 2009.

Stuxnet: A New Era of Cyberwarfare

Stuxnet may be the most notorious known act of cyberwarfare effort to date (one expert called it "the most sophisticated worm ever created").N. Firth, "Computer Super-Virus 'Targeted Iranian Nuclear Power Station' but Who Made It?" *Daily Mail*, September 24, 2010. Suspected to have been launched by either U.S. or Israeli intelligence (or both), Stuxnet infiltrated Iranian nuclear facilities and reprogramed the industrial control software operating hundreds of uranium-enriching centrifuges. The worm made the devices spin so fast that the centrifuges effectively destroyed themselves, in the process setting back any Iranian nuclear ambitions. The attack was so sophisticated that it even altered equipment readings to report normal activity so that operators didn't even know something was wrong until it was too late.

Some might fear Stuxnet in the wild—what happens if the code spread to systems operated by peaceful nations or systems controlling critical infrastructure that could threaten lives if infected? All important questions, but in Stuxnet's case the worm appears to have been designed to target very specific systems. If it got onto a nontarget machine, it would become inert. Propagation was also limited, with each copy designed to infect only three additional machines. And the virus was also designed to self-destruct at a future date.M. Gross, "A Declaration of Cyber-War," *Vanity Fair*, April 2011.

Stuxnet showed that with computers at the heart of so many systems, it's now possible to destroy critical infrastructure without firing a shot.T. Butterworth, "The War against Iran Has Already Started," *Forbes*. September 21, 2010. While few want to see Iran get the bomb, what does the rise of cyberwarfare mean for future combat and for citizen vulnerability, and what might this mean for businesses whose products, services, or organizations may become targets?

Other threats come from malicious pranksters (sometimes called *griefers* or *trolls*), like the group that posted seizure-inducing images on Web sites frequented by epilepsy sufferers.M. Schwartz, "The Trolls among Us," *New York Times*, August 3, 2008. Others are **hacktivists**[5], targeting firms, Web sites, or even users as a protest measure. In 2009, Twitter was brought down and Facebook and LiveJournal were hobbled as Russian-sympathizing hacktivists targeted the social networking and blog accounts of the Georgian blogger known as Cyxymu. The silencing of millions of accounts was simply collateral damage in a massive DDoS attack meant to mute

5. A protester seeking to make a political point by leveraging technology tools, often through system infiltration, defacement, or damage.

this single critic of the Russian government.J. Schectman, "Computer Hacking Made Easy," *BusinessWeek*, August 13, 2009.

And as power and responsibility is concentrated in the hands of a few revenge-seeking employees can do great damage. The San Francisco city government lost control of a large portion of its own computer network over a ten-day period when a single disgruntled employee refused to divulge critical passwords.J. Vijayan, "After Verdict, Debate Rages in Terry Childs Case," *Computerworld*, April 28, 2010.

The bad guys are legion and the good guys often seem outmatched and underresourced. Law enforcement agencies dealing with computer crime are increasingly outnumbered, outskilled, and underfunded. Many agencies are staffed with technically weak personnel who were trained in a prior era's crime fighting techniques. Governments can rarely match the pay scale and stock bonuses offered by private industry. Organized crime networks now have their own R&D labs and are engaged in sophisticated development efforts to piece together methods to thwart current security measures.

"Hacker": Good or Bad?

The terms **hacker**[6] and **hack**[7] are widely used, but their meaning is often based on context. When referring to security issues, the media widely refers to hackers as bad guys who try to break into (hack) computer systems. Some geezer geeks object to this use, as the term *hack* in computer circles originally referred to a clever (often technical) solution and the term *hacker* referred to a particularly skilled programmer. Expect to see the terms used both positively and negatively.

You might also encounter the terms **white hat hackers**[8] and **black hat hackers**[9]. The white hats are the good guys who probe for weaknesses, but don't exploit them. Instead, they share their knowledge in hopes that the holes they've found will be plugged and security will be improved. Many firms hire consultants to conduct "white hat" hacking expeditions on their own assets as part of their auditing and security process. "Black hats" are the bad guys. Some call them "crackers." There's even a well-known series of hacker conventions known as the Black Hat conference.

6. A term that, depending on the context, may be applied to either 1) someone who breaks into computer systems, or 2) to a particularly clever programmer.
7. A term that may, depending on the context, refer to either 1) breaking into a computer system, or 2) a particularly clever solution.
8. Someone who uncovers computer weaknesses without exploiting them. The goal of the white hat hacker is to improve system security.
9. A computer criminal.

KEY TAKEAWAYS

- Computer security threats have moved beyond the curious teen with a PC and are now sourced from a number of motivations, including theft, leveraging compromised computing assets, extortion, espionage, warfare, terrorism, pranks, protest, and revenge.
- Threats can come from both within the firm as well as from the outside.
- Cybercriminals operate in an increasingly sophisticated ecosystem where data harvesters and tool peddlers leverage sophisticated online markets to sell to cash-out fraudsters and other crooks.
- Technical and legal complexity make pursuit and prosecution difficult.
- Many law enforcement agencies are underfunded, underresourced, and underskilled to deal with the growing hacker threat.

QUESTIONS AND EXERCISES

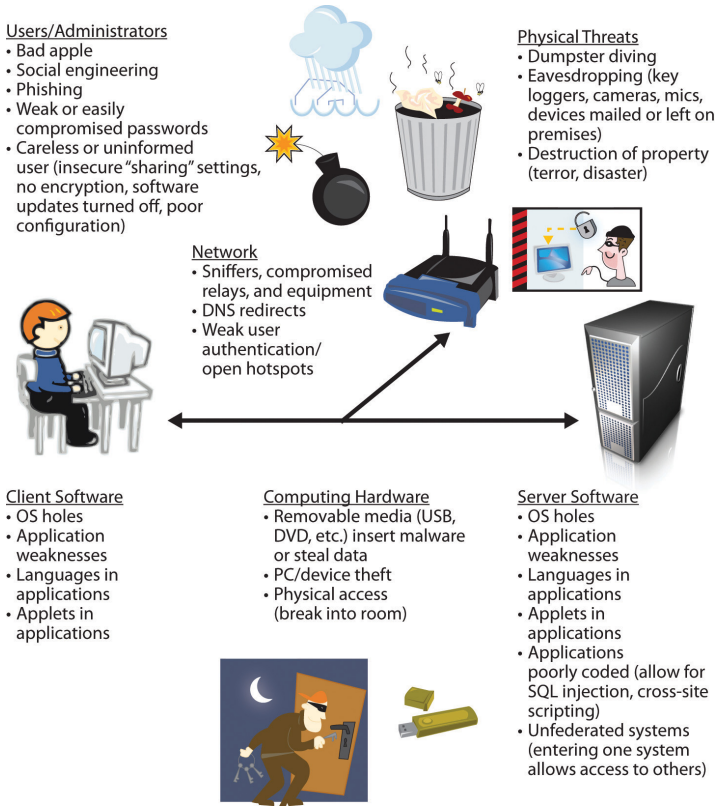
1. What is a botnet? What sorts of exploits would use a botnet? Why would a botnet be useful to cybercriminals?
2. Why are threats to the power grid potentially so concerning? What are the implications of power-grid failure and of property damage? Who might execute these kinds of attacks? What are the implications for firms and governments planning for the possibility of cyberwarfare and cyberterror?
3. Scan the trade press for examples of hacking that apply to the various motivations mentioned in this chapter. What happened to the hacker? Were they caught? What penalties do they face?
4. Why do cybercriminals execute attacks across national borders? What are the implications for pursuit, prosecution, and law enforcement?
5. Why do law enforcement agencies struggle to cope with computer crime?
6. A single rogue employee effectively held the city of San Francisco's network hostage for ten days. What processes or controls might the city have created that could have prevented this kind of situation from taking place?
7. The Geneva Conventions are a set of international treaties that in part set standards for protecting citizens in and around a war zone. Should we have similar rules that set the limits of cyberwarfare? Would such limits even be effective? Why or why not?
8. What does the rise of cyberwarfare suggest for businesses and organizations? What sorts of contingencies should firms consider and possibly prepare for? How might considerations also impact a firm's partners, customers, and suppliers?

13.3 Where Are Vulnerabilities? Understanding the Weaknesses

LEARNING OBJECTIVES

1. Recognize the potential entry points for security compromise.
2. Understand infiltration techniques such as social engineering, phishing, malware, Web site compromises (such as SQL injection), and more.
3. Identify various methods and techniques to thwart infiltration.

Figure 13.1



This diagram shows only some of the potential weaknesses that can compromise the security of an organization's information systems. Every physical or network "touch point" is a potential vulnerability. Understanding where weaknesses may exist is a vital step toward improved security.

Source: http://office.microsoft.com/en-us/clipart/default.aspx

Modern information systems have lots of interrelated components and if one of these components fails, there might be a way in to the goodies. This creates a large attack surface for potential infiltration and compromise, as well as one that is simply vulnerable to unintentional damage and disruption.

User and Administrator Threats

Bad Apples

While some of the more sensational exploits involve criminal gangs, research firm Gartner estimates that 70 percent of loss-causing security incidents involve insiders.J. Mardesich, "Ensuring the Security of Stored Data," CIO Strategy Center, 2009. Rogue employees can steal secrets, install malware, or hold a firm hostage. Check processing firm Fidelity National Information Services was betrayed when one of its database administrators lifted personal records on 2.3 million of the firm's customers and illegally sold them to direct marketers.

And it's not just firm employees. Many firms hire temporary staffers, contract employees, or outsource key components of their infrastructure. Other firms have been compromised by members of their cleaning or security staff. A contract employee working at Sentry Insurance stole information on 110,000 of the firm's clients.J. Vijayan, "Software Consultant Who Stole Data on 110,000 People Gets Five-Year Sentence," *Computerworld*, July 10, 2007.

Social Engineering

As P. T. Barnum is reported to have said, "There's a sucker born every minute." Con games that trick employees into revealing information or performing other tasks that compromise a firm are known as *social engineering* in security circles. In some ways, crooks have never had easier access to background information that might be used to craft a scam. It's likely that a directory of a firm's employees, their titles, and other personal details is online right now via social networks like LinkedIn and Facebook. With just a few moments of searching, a skilled con artist can piece together a convincing and compelling story.

A Sampling of Methods Employed in Social Engineering

- Impersonating senior management, a current or new end user needing help with access to systems, investigators, or staff (fake uniforms, badges)
- Identifying a key individual by name or title as a supposed friend or acquaintance
- Making claims with confidence and authority ("Of course I belong at this White House dinner.")
- Baiting someone to add, deny, or clarify information that can help an attacker
- Using harassment, guilt, or intimidation
- Using an attractive individual to charm others into gaining information, favors, or access
- Setting off a series of false alarms that cause the victim to disable alarm systems
- Answering bogus surveys (e.g., "Win a free trip to Hawaii—just answer three questions about your network.")

Data aggregator ChoicePoint sold private information to criminals who posed as legitimate clients, compromising the names, addresses, and Social Security numbers of some 145,000 individuals. In this breach, not a single computer was compromised. Employees were simply duped into turning data over to crooks. Gaffes like that can be painful. ChoicePoint paid $15 million in a settlement with the Federal Trade Commission, suffered customer loss, and ended up abandoning once lucrative businesses.G. Anthes, "The Grill: Security Guru Ira Winkler Takes the Hot Seat," *Computerworld*, July 28, 2008.

Phishing

Phishing[10] refers to cons executed through technology. The goal of phishing is to leverage the reputation of a trusted firm or friend to trick the victim into performing an action or revealing information. The cons are crafty. Many have masqueraded as a security alert from a bank or e-commerce site ("Our Web site has been compromised, click to log in and reset your password."), a message from an employer, or even a notice from the government ("Click here to update needed information to receive your tax refund transfer."). Sophisticated con artists will lift logos, mimic standard layouts, and copy official language from legitimate Web sites or prior e-mails. Gartner estimates that these sorts phishing attacks cost consumers

10. A con executed using technology, typically targeted at acquiring sensitive information or tricking someone into installing malicious software.

$3.2 billion in 2007.L. Avivah, “Phishing Attacks Escalate, Morph, and Cause Considerable Damage,” *Gartner*, December 12, 2007.

Other phishing attempts might dupe a user into unwittingly downloading dangerous software (malware) that can do things like record passwords and keystrokes, provide hackers with deeper access to your corporate network, or enlist your PC as part of a botnet. One attempt masqueraded as a message from a Facebook friend, inviting the recipient to view a video. Victims clicking the link were then told they need to install an updated version of the Adobe Flash plug-in to view the clip. The plug in was really a malware program that gave phishers control of the infected user’s computer.B. Krebs, “‘Koobface’ Worm Resurfaces on Facebook, MySpace,” *Washington Post*, March 2, 2009. Other attempts have populated P2P networks (peer-to-peer file distribution systems such as BitTorrent) with malware-installing files masquerading as video games or other software, movies, songs, and pornography.

So-called spear phishing attacks specifically target a given organization or group of users. In one incident, employees of a medical center received e-mails purportedly from the center itself, indicating that the recipient was being laid off and offering a link to job counseling resources. The link really offered a software payload that recorded and forwarded any keystrokes on the victim’s PC.C. Garretson, “Spam that Delivers a Pink Slip,” *NetworkWorld*, November 1, 2006. And with this type of phishing, the more you know about a user, the more convincing it is to con them. Phishers using pilfered résumé information from Monster.com crafted targeted and personalized e-mails. The request, seemingly from the job site, advised users to download the “Monster Job Seeker Tool”; this “tool” installed malware that encrypted files on the victim’s PC, leaving a ransom note demanding payment to liberate a victim’s hard disk.T. Wilson, “Trojan On Monster.com Steals Personal Data,” *Forbes*, August 20, 2007.

Don’t Take the Bait: Recognizing the “Phish Hooks”

Web browser developers, e-mail providers, search engines, and other firms are actively working to curtail phishing attempts. Many firms create blacklists that block access to harmful Web sites and increasingly robust tools screen for common phishing tactics. But it’s still important to have your guard up. Some exploits may be so new that they haven’t made it into screening systems (so-called zero-day exploits).

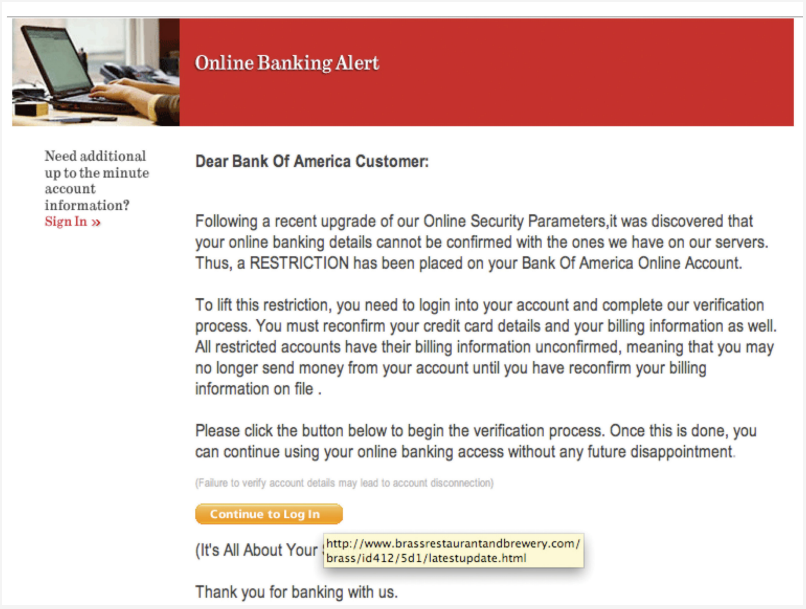
Never click on a link or download a suspicious, unexpected enclosure without verifying the authenticity of the sender. If something looks suspicious, don’t implicitly trust the “from” link in an e-mail. It’s possible that the e-mail address has been **spoofed**[11] (faked) or that it was sent via a colleague’s compromised account. If unsure, contact the sender or your security staff.

Also know how to read the complete URL to look for tricks. Some firms misspell Web address names (http://wwwyourbank.com—note the missing period), set up subdomains to trick the eye (http://yourbank.com.sneakysite.com—which is hosted at sneakysite.com even though a quick glance looks like yourbank.com), or hijack brands by registering a legitimate firm’s name via foreign top-level domains (http://yourbank.cn).

A legitimate URL might also appear in a phishing message, but an HTML coding trick might make something that looks like http://yourbank.com/login actually link to http://sneakysite.com. Hovering your cursor over the URL or an image connected to a link should reveal the actual URL as a tool tip (just don’t click it, or you’ll go to that site).

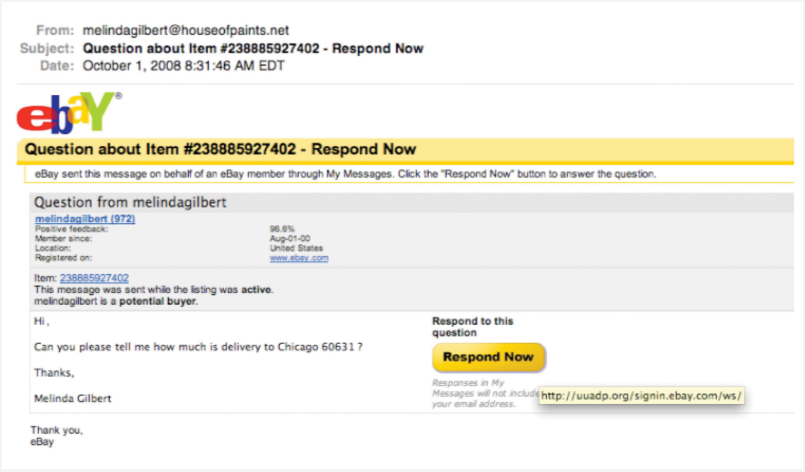
11. Term used in security to refer to forging or disguising the origin or identity. E-mail transmissions and packets that have been altered to seem as if they came from another source are referred to as being “spoofed.”

Figure 13.2



This e-mail message looks like it's from Bank of America. However, hovering the cursor above the "Continue to Log In" button reveals the URL without clicking through to the site. Note how the actual URL associated with the link is not associated with Bank of America.

Figure 13.3



This image is from a phishing scheme masquerading as an eBay message. The real destination is a compromised .org domain unassociated with eBay, but the phishers have created a directory at this domain named "signin.ebay.com" in hopes that users will focus on that part of the URL and not recognize they're really headed to a non-eBay site.

Web 2.0: The Rising Security Threat

Social networks and other Web 2.0 tools are a potential gold mine for crooks seeking to pull off phishing scams. Malware can send messages that seem to come from trusted "friends." Messages such as status updates and tweets are short, and with limited background information, there are fewer contexts to question a post's validity. Many users leverage bit.ly or other URL-shortening services that don't reveal the Web site they link to in their URL, making it easier to hide a malicious link. While the most popular URL-shortening services maintain a blacklist, early victims are threatened by **zero-day exploits**[12]. Criminals have also been using a variety of techniques to spread malware across sites or otherwise make them difficult to track and catch.

The technical openness of many Web 2.0 efforts can also create problems if schemes aren't implemented properly. For example, Mark Zuckerberg's Facebook page fell victim to hackers who used a hole in a Facebook API that allowed unauthorized status update posts to public Facebook fan pages.G. Cluley, "Mark Zuckerberg Fan Page Hacked on Facebook: What Really Happened?" *NakedSecurity*, January 27, 2011. APIs can allow firms to share services, collaborate, and enable mash-ups, but if code is poorly implemented it can also be an open back door where the bad guys can sneak in.

Some botnets have even used Twitter to communicate by sending out coded tweets to instruct compromised machines.UnsafeBits, "Botnets Go Public by Tweeting on Twitter," *Technology Review*, August 17, 2009. Social media can also be a megaphone for loose lips, enabling a careless user to broadcast proprietary information to the public domain. A 2009 Congressional delegation to Iraq was supposed to have been secret. But Rep. Peter Hoekstra tweeted his final arrival into Baghdad for all to see, apparently unable to contain his excitement at receiving BlackBerry service in Iraq. Hoekstra tweeted, "Just landed in Baghdad. I believe it may be first time I've had bb service in Iraq. 11th trip here." You'd think he would have known better. At the time, Hoekstra was a ranking member of the House Intelligence Committee!

12. Attacks that are so new that they haven't been clearly identified, and so they haven't made it into security screening systems.

Figure 13.4

A member of the House Intelligence Committee uses Twitter and reveals his locale on a secret trip.

Passwords

Many valuable assets are kept secure via just one thin layer of protection—the password. And if you're like most users, your password system is a mess.F. Manjoo, "Fix Your Terrible, Insecure Passwords in Five Minutes," *Slate*, November 12, 2009. With so many destinations asking for passwords, chances are you're using the same password (or easily guessed variants) in a way that means getting just one "key" would open many "doors." The typical Web user has 6.5 passwords, each of which is used at four sites, on average.N. Summers, "Building a Better Password," *Newsweek*, October 19, 2009. Some sites force users to change passwords regularly, but this often results in insecure compromises. Users make only minor tweaks (e.g., appending the month or year); they write passwords down (in an unlocked drawer or Post-it note attached to the monitor); or they save passwords in personal e-mail accounts or on unencrypted hard drives.

The challenge questions offered by many sites to automate password distribution and reset are often pitifully insecure. What's your mother's maiden name? What elementary school did you attend? Where were you born? All are pretty easy to guess. One IEEE study found acquaintances could correctly answer colleagues' secret questions 28 percent of the time, and those who did not know the person still guessed right at a rate of 17 percent. Plus, within three to six months, 16 percent of study participants forgot answers to *their own* security questions.R. Lemos, "Are Your 'Secret Questions' Too Easily Answered?" *Technology Review*, May 18, 2009. In many cases, answers to these questions can be easily uncovered online. Chances are, if you've got an account at a site like Ancestry.com, classmates.com, or Facebook, then some of your secret answers have already been exposed—by you! A

Tennessee teen hacked into Sarah Palin's personal Yahoo! account (gov.palin@yahoo.com) in part by correctly guessing where she met her husband. A similar attack hit staffers at Twitter, resulting in the theft of hundreds of internal documents, including strategy memos, e-mails, and financial forecasts, many of which ended up embarrassingly posted online.N. Summers, "Building a Better Password," *Newsweek*, October 19, 2009.

Related to the password problem are issues with system setup and configuration. Many vendors sell software with a common default password. For example, for years, leading database products came with the default account and password combination "scott/tiger." Any firm not changing default accounts and passwords risks having an open door. Other firms are left vulnerable if users set systems for open access—say turning on file sharing permission for their PC. Programmers, take note: well-designed products come with secure default settings, require users to reset passwords at setup, and also offer strong warnings when security settings are made weaker. But unfortunately, there are a lot of legacy products out there, and not all vendors have the insight to design for out-of-the-box security.

Building a Better Password

There's no simple answer for the password problem. **Biometrics**[13] are often thought of as a solution, but technologies that replace conventionally typed passwords with things like fingerprint readers, facial recognition, or iris scans are still rarely used, and PCs that include such technologies are widely viewed as novelties. Says Carnegie Mellon University CyLab fellow Richard Power, "Biometrics never caught on and it never will."N. Summers, "Building a Better Password," *Newsweek*, October 19, 2009.

Other approaches leverage technology that distributes single use passwords. These might arrive via external devices like an electronic wallet card, key chain fob, or cell phone. Security firm RSA has even built the technology into BlackBerrys. Enter a user name and receive a phone message with a temporary password. Even if a system was compromised by keystroke capture malware, the password is only good for one session. Lost device? A central command can disable it. This may be a good solution for situations that demand a high level of security, and Wells Fargo and PayPal are among the firms offering these types of services as an option. However, for most consumer applications, slowing down users with a two-tier authentication system would be an impractical mandate.

While you await technical fixes, you can at least work to be part of the solution rather than part of the problem. It's unlikely you've got the memory or discipline to create separate unique passwords for all of your sites, but at least make it a priority to create separate, hard-to-guess passwords for each of your highest priority accounts (e.g., e-mail, financial Web sites, corporate network, and PC). Remember, the integrity of a password shared across Web sites isn't just up to you. That hot start-up Web service may not have the security resources or experience to protect your special code, and if that Web site's account is hacked, your user name and password are now in the hands of hackers that can try out those "keys" across the Web's most popular destinations.

Web sites are increasingly demanding more "secure" passwords, requiring users to create passwords at least eight characters in length and that include at least one number and other nonalphabet character. Beware of using seemingly clever techniques to disguise common words. Many commonly available brute-force password cracking tools run through dictionary guesses of common

13. Technologies that measure and analyze human body characteristics for identification or authentication. These might include fingerprint readers, retina scanners, voice and face recognition, and more.

words or phrases, substituting symbols or numbers for common characters (e.g., “@” for “a,” “+” for “t”). For stronger security, experts often advise basing passwords on a phrase, where each letter makes up a letter in an acronym. For example, the phrase “My first Cadillac was a real lemon so I bought a Toyota” becomes “M1stCwarlsIbaT.”F. Manjoo, “Fix Your Terrible, Insecure Passwords in Five Minutes,” *Slate*, November 12, 2009. Be careful to choose an original phrase that’s known only by you and that’s easy for you to remember. Studies have shown that acronym-based passwords using song lyrics, common quotes, or movie lines are still susceptible to dictionary-style hacks that build passwords from pop-culture references (in one test, two of 144 participants made password phrases from an acronym of the Oscar Meyer wiener jingle).N. Summers, “Building a Better Password,” *Newsweek*, October 19, 2009. Finding that balance between something tough for others to guess yet easy for you to remember will require some thought—but it will make you more secure. Do it now!

Technology Threats (Client and Server Software, Hardware, and Networking)

Malware

Any accessible computing device is a potential target for infiltration by malware. *Malware* (for malicious software) seeks to compromise a computing system without permission. Client PCs and a firm’s servers are primary targets, but as computing has spread, malware now threatens nearly any connected system running software, including mobile phones, embedded devices, and a firm’s networking equipment.

Some hackers will try to sneak malware onto a system via techniques like phishing. In another high-profile hacking example, infected USB drives were purposely left lying around government offices. Those seemingly abandoned office supplies really contained code that attempted to infiltrate government PCs when inserted by unwitting employees.

Machines are constantly under attack. Microsoft’s Internet Safety Enforcement Team claims that the mean time to infection for an unprotected PC is less than five minutes.J. Markoff, “A Robot Network Seeks to Enlist Your Computer,” *New York Times*, October 20, 2008. Oftentimes malware attempts to compromise weaknesses in software—either bugs, poor design, or poor configuration.

Years ago, most attacks centered on weaknesses in the operating system, but now malware exploits have expanded to other targets, including browsers, plug-ins, and scripting languages used by software. *BusinessWeek* reports that Adobe has replaced Microsoft as the primary means by which hackers try to infect or take control of PCs. Even trusted Web sites have become a conduit to deliver malware payloads. More than a dozen sites, including those of the *New York Times*, *USA Today*, and *Nature*, were compromised when seemingly honest advertising clients switched on fake ads that exploit Adobe software.A. Ricadela, "Can Adobe Beat Back the Hackers?" *BusinessWeek*, November 19, 2009. Some attacks were delivered through Flash animations that direct computers to sites that scan PCs, installing malware payloads through whatever vulnerabilities are discovered. Others circulated via e-mail through PDF triggered payloads deployed when a file was loaded via Acrobat Reader. Adobe is a particularly tempting target, as Flash and Acrobat Reader are now installed on nearly every PC, including Mac and Linux machines.

Malware goes by many names. Here are a few of the more common terms you're likely to encounter.Portions adapted from G. Perera, "Your Guide to Understanding Malware," *LaptopLogic.com*, May 17, 2009.

Methods of infection are as follows:

- *Viruses.* Programs that infect other software or files. They require an executable (a running program) to spread, attaching to other executables. Viruses can spread via operating systems, programs, or the boot sector or auto-run feature of media such as DVDs or USB drives. Some applications have executable languages (macros) that can also host viruses that run and spread when a file is open.
- *Worms.* Programs that take advantage of security vulnerability to automatically spread, but unlike viruses, worms do not require an executable. Some worms scan for and install themselves on vulnerable systems with stunning speed (in an extreme example, the SQL Slammer worm infected 90 percent of vulnerable software worldwide within just ten minutes).M. Broersma, "Slammer—the First 'Warhol' Worm?" *CNET*, February 3, 2003.
- *Trojans.* Exploits that, like the mythical Trojan horse, try to sneak in by masquerading as something they're not. The payload is released when the user is duped into downloading and installing the malware cargo, oftentimes via phishing exploits.

While the terms above cover methods for infection, the terms below address the goal of the malware:

- *Botnets or zombie networks.* Hordes of surreptitiously infected computers linked and controlled remotely by a central command. Botnets are used in crimes where controlling many difficult-to-identify PCs is useful, such as when perpetrating click fraud, sending spam, registering accounts that use **CAPTCHAs**[14]G. Keizer, "Botnet Busts Newest Hotmail CAPTCHA," *Computerworld*, February 19, 2009. (those scrambled character images meant to thwart things like automated account setup or ticket buying), executing "dictionary" password cracking attempts, or launching denial-of-service attacks.
- *Malicious adware.* Programs installed without full user consent or knowledge that later serve unwanted advertisements.
- *Spyware.* Software that surreptitiously monitors user actions, network traffic, or scans for files.
- *Keylogger.* Type of spyware that records user keystrokes. Keyloggers can be either software-based or hardware, such as a recording "dongle" that is plugged in between a keyboard and a PC.
- *Screen capture.* Variant of the keylogger approach. This category of software records the pixels that appear on a user's screen for later playback in hopes of identifying proprietary information.
- *Blended threats.* Attacks combining multiple malware or hacking exploits.

14. An acronym for Completely Automated Public Turing Test to Tell Computers and Humans Apart. CAPTCHAs are those scrambled character images that many sites require to submit some sort of entry (account setup, ticket buying). CAPTCHAs were developed because computers have difficulty discerning letters that are distorted or mixed inside a jumbled graphic. CAPTCHAs are meant to be a *Turing Test*—a test to distinguish if a task is being performed by a computer or a human.

All the News Fit to Print (Brought to You by Scam Artists)

In fall 2009, bad guys posing as the telecom firm Vonage signed up to distribute ads through the *New York Times* Web site. Many firms that display online ads on their Web sites simply create placeholders on their Web pages, with the actual ad content served by the advertisers themselves (see Chapter 14 "Google in Three Parts: Search, Online Advertising, and Beyond" for details). In this particular case, the scam artists posing as Vonage switched off the legitimate-looking ads and switched on code that, according to the *New York Times*, "took over the browsers of many people visiting the site, as their screens filled with an image that seemed to show a scan for computer viruses. The visitors were then told that they needed to buy antivirus software to fix a problem, but the software was more snake oil than a useful program."A. Vance, "Times Web Ads Show Security Breach," *New York Times*, September 14, 2009. Sites ranging from Fox News, the *San Francisco Chronicle*, and British tech site The Register have also been hit with ad scams in the past. In the *Times* case, malware wasn't distributed directly to user PCs, but by passing through ads from third parties to consumers, the *Times* became a conduit for a scam. In the same way that manufacturers need to audit their supply chain to ensure that partners aren't engaged in sweatshop labor or disgraceful pollution, sites that host ads need to audit their partners to ensure they are legitimate and behaving with integrity.

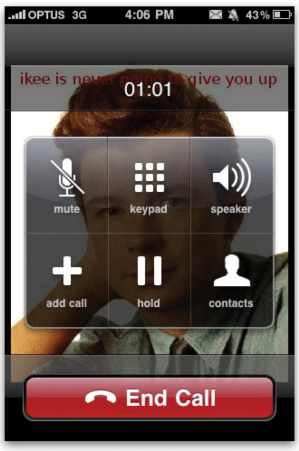
The Virus in Your Pocket

Most mobile phones are really pocket computers, so it's not surprising that these devices have become malware targets. And there are a lot of pathways to exploit. Malware might infiltrate a smartphone via e-mail, Internet surfing, MMS attachments, or even Bluetooth. The "commwarrior" mobile virus spread to at least eight countries, propagating from a combination of MMS messages and Bluetooth.J. Charney, "Commwarrior Cell Phone Virus Marches On," *CNET*, June 5, 2005.

Most smartphones have layers of security to block the spread of malware, so hackers typically hunt for the weakest victims. Easy marks include "jail-broken" iPhones, devices with warranty-voiding modifications in which security restrictions are overridden to allow phones to be used off network, and for the installation of unsanctioned applications. Estimates suggest some 10 percent of iPhones are jail-broken, and early viruses exploiting the compromised devices ranged from a "Rick roll" that replaced the home screen image with a photo of 1980s crooner Rick AstleyS. Steade, "It's Shameless How They Flirt," *Good Morning Silicon Valley*, November 9, 2009. to the more nefarious Ikee.B, which scanned text messages and hunted out banking codes, forwarding the nabbed data to a server in Lithuania.R. Lemos, "Nasty iPhone Worm Hints at the Future," *Technology Review*, November 29, 2009.

The upside? Those smart devices are sometimes crime fighters themselves. A Pittsburgh mugging victim turned on Apple's "Find My iPhone" feature within its MobileMe service, mapping the perpetrator's path, then sending the law to bust the bad guys while they ate at a local restaurant.J. Murrell, "The iWitness News Roundup: Crime-fighting iPhone," *Good Morning Silicon Valley*, August 31, 2009.

Figure 13.5



A "jail-broken" iPhone gets "Rick rolled" by malware.

Compromising Web Sites

Some exploits directly target poorly designed and programmed Web sites. Consider the SQL injection technique. It zeros in on a sloppy programming practice where software developers don't validate user input.

It works like this. Imagine that you visit a Web site and are asked to enter your user ID in a field on a Web page (say your user ID is smith). A Web site may be programmed to take the data you enter from the Web page's user ID field (smith), then add it to a database command (creating the equivalent of a command that says "find the account for 'smith'"). The database then executes that command.

But Web sites that don't verify user entries and instead just blindly pass along entered data are vulnerable to attack. Hackers with just a rudimentary knowledge of SQL could type actual code fragments into the user ID field, appending this code to statements executed by the site (see sidebar for a more detailed description). Such modified instructions could instruct the Web site's database software to drop (delete) tables, insert additional data, return all records in a database, or even redirect users to another Web site that will scan clients for weaknesses, then launch further attacks. Security expert Ben Schneier noted a particularly ghastly SQL injection vulnerability in the publicly facing database for the Oklahoma Department

of Corrections, where "anyone with basic SQL knowledge could have registered anyone he wanted as a sex offender."B. Schneier, "Oklahoma Data Leak," *Schneier on Security*, April 18, 2008.

Not trusting user input is a cardinal rule of programming, and most well-trained programmers know to validate user input. But there's a lot of sloppy code out there, which hackers are all too eager to exploit. IBM identifies SQL injection as the fastest growing security threat, with over half a million attack attempts recorded each day.A. Wittmann, "The Fastest-Growing Security Threat," *InformationWeek*, November 9, 2009. Some vulnerable systems started life as quickly developed proofs of concepts, and programmers never went back to add the needed code to validate input and block these exploits. Other Web sites may have been designed by poorly trained developers who have moved on to other projects, by staff that have since left the firm, or where development was outsourced to another firm. As such, many firms don't even know if they suffer from this vulnerability.

SQL injection and other application weaknesses are particularly problematic because there's not a commercial software patch or easily deployed piece of security software that can protect a firm. Instead, firms have to meticulously examine the integrity of their Web sites to see if they are vulnerable.While some tools exist to automate testing, this is by no means as easy a fix as installing a commercial software patch or virus protection software.

How SQL Injection Works

For those who want to get into some of the geekier details of a SQL injection attack, consider a Web site that executes the code below to verify that an entered user ID is in a database table of usernames. The code executed by the Web site might look something like this:

"SELECT * FROM users WHERE userName = '" + userID + "';"

The statement above tells the database to SELECT (find and return) all columns (that's what the "*" means) from a table named users where the database's userName field equals the text you just entered in the userID field. If the Web site's visitor entered smith, that text is added to the statement above, and it's executed as:

"SELECT * FROM users WHERE userName = 'smith';"

No problem. But now imagine a hacker gets sneaky and instead of just typing smith, into the Web site's userID field, they also add some *additional* SQL code like this:

smith'; DROP TABLE users; DELETE * FROM users WHERE 't' = 't

If the programming statement above is entered into the user ID, the Web site adds this code to its own programming to create a statement that is executed as:

SELECT * FROM users WHERE userName = 'smith'; DELETE * FROM users WHERE 't' = 't';

The semicolons separate SQL statements. That second statement says delete all data in the users table for records where 't' = 't' (this last part, 't' = 't,' is always true, so all records will be deleted). Yikes! In this case, someone entering the kind of code you'd learn in the first chapter of *SQL for Dummies* could annihilate a site's entire user ID file using one of the site's own Web pages as the attack vehicle.B. Schneier, "Oklahoma Data Leak," *Schneier on Security*, April 18, 2008.

Related programming exploits go by names such as cross-site scripting attacks and HTTP header injection. We'll spare you the technical details, but what this means for both the manager and the programmer is that all systems must be designed and tested with security in mind. This includes testing new applications, existing and legacy applications, partner offerings, and SaaS (software as a service) applications—everything. Visa and MasterCard are among the firms requiring partners to rigorously apply testing standards. Firms that aren't testing their applications will find they're locked out of business; if caught with unacceptable breaches, such firms may be forced to pay big fines and absorb any costs associated with their weak practices."Information Security: Why Cybercriminals Are Smiling," *Knowledge@Wharton*, August 19, 2009.

Push-Button Hacking

Not only are the list of technical vulnerabilities well known, hackers have created tools to make it easy for the criminally inclined to automate attacks. Chapter 14 "Google in Three Parts: Search, Online Advertising, and Beyond" outlines how Web sites can interrogate a system to find out more about the software and hardware used by visitors. Hacking toolkits can do the same thing. While you won't find this sort of software for sale on Amazon, a casual surfing of the online underworld (not recommended or advocated) will surface scores of tools that probe systems for the latest vulnerabilities then launch appropriate attacks. In one example, a $700 toolkit (MPack v. 86) was used to infiltrate a host of Italian Web sites, launching Trojans that infested 15,000 users in just a six-day period."Web Threats Whitepaper," *Trend Micro*, March 2008. As an industry executive in *BusinessWeek* has stated, "The barrier of entry is becoming so low that literally anyone can carry out these attacks."J. Schectman, "Computer Hacking Made Easy," *BusinessWeek*, August 13, 2009.

Network Threats

The network itself may also be a source of compromise. Recall that the TJX hack happened when a Wi-Fi access point was left open and undetected. A hacker just drove up and performed the digital equivalent of crawling through an open window. The problem is made more challenging since wireless access points are so inexpensive and easy to install. For less than $100, a user (well intentioned or not) could plug in to an access point that could provide entry for anyone. If a firm doesn't regularly monitor its premises, its network, and its network traffic, it may fall victim.

Other troubling exploits have targeted the very underpinning of the Internet itself. This is the case with so-called DNS cache poisoning. The DNS, or domain name service, is a collection of software that maps an Internet address, such as

(http://www.bc.edu), to an IP address, such as 136.167.2.220. 220 (see Chapter 12 "A Manager's Guide to the Internet and Telecommunications" for more detail). DNS cache poisoning exploits can redirect this mapping and the consequences are huge. Imagine thinking that you're visiting your bank's Web site, but instead your network's DNS server has been poisoned so that you really visit a carefully crafted replica that hackers use to steal your log-in credentials and drain your bank account. A DNS cache poisoning attack launched against one of China's largest ISPs redirected users to sites that launched malware exploits, targeting weaknesses in RealPlayer, Adobe Flash, and Microsoft's ActiveX technology, commonly used in browsers.J. London, "China Netcom Falls Prey to DNS Cache Poisoning," *Computerworld*, August 22, 2008.

Physical Threats

A firm doesn't just have to watch out for insiders or compromised software and hardware; a host of other physical threats can grease the skids to fraud, theft, and damage. Most large firms have disaster-recovery plans in place. These often include provisions to backup systems and data to off-site locales, to protect operations and provide a fall back in the case of disaster. Such plans increasingly take into account the potential impact of physical security threats such as terrorism, or vandalism, as well.

Anything valuable that reaches the trash in a recoverable state is also a potential security breach. Hackers and spies sometimes practice **dumpster diving**[15], sifting through trash in an effort to uncover valuable data or insights that can be stolen or used to launch a security attack. This might include hunting for discarded passwords written on Post-it notes, recovering unshredded printed user account listings, scanning e-mails or program printouts for system clues, recovering tape backups, resurrecting files from discarded hard drives, and more.

Other compromises might take place via **shoulder surfing**[16], simply looking over someone's shoulder to glean a password or see other proprietary information that might be displayed on a worker's screen.

Firms might also fall victim to various forms of eavesdropping, such as efforts to listen into or record conversations, transmissions, or keystrokes. A device hidden inside a package might sit inside a mailroom or a worker's physical inbox, scanning for open wireless connections, or recording and forwarding conversations.J. Robertson, "Hackers Mull Physical Attacks on a Networked World," *San Francisco Chronicle*, August 8, 2008. Other forms of eavesdropping can be accomplished via compromised wireless or other network connections, malware keylogger or screen capture programs, as well as hardware devices such as replacement keyboards with

15. Combing through trash to identify valuable assets.

16. Gaining compromising information through observation (as in looking over someone's shoulder).

keyloggers embedded inside, microphones to capture the slightly unique and identifiable sound of each key being pressed, programs that turn on built-in microphone or cameras that are now standard on many PCs, or even James Bond-style devices using Van Eck techniques that attempt to read monitors from afar by detecting their electromagnetic emissions.

The Encryption Prescription

During a routine physical transfer of backup media, Bank of America lost tapes containing the private information—including Social Security and credit card numbers—of hundreds of thousands of customers.J. Mardesich, "Ensuring the Security of Stored Data," CIO Strategy Center, 2009. This was potentially devastating fodder for identity thieves. But who cares if someone steals your files if they still can't read the data? That's the goal of encryption!

Encryption[17] scrambles data, making it essentially unreadable to any program that doesn't have the descrambling password, known as a **key**[18]. Simply put, the larger the key, the more difficult it is for a brute-force attack to exhaust all available combinations and crack the code. When well implemented, encryption can be the equivalent of a rock solid vault. To date, the largest known **brute-force attacks**[19], demonstration hacks launched by grids of simultaneous code-cracking computers working in unison, haven't come close to breaking the type of encryption used to scramble transmissions that most browsers use when communicating with banks and shopping sites. The problem occurs when data is nabbed before encryption or after decrypting, or in rare cases, if the encrypting key itself is compromised.

Extremely sensitive data—trade secrets, passwords, credit card numbers, and employee and customer information—should be encrypted before being sent or stored.J. Mardesich, "Ensuring the Security of Stored Data," CIO Strategy Center, 2009. Deploying encryption dramatically lowers the potential damage from lost or stolen laptops, or from hardware recovered from dumpster diving. It is vital for any laptops carrying sensitive information.

Encryption is also employed in virtual private network (VPN) technology, which scrambles data passed across a network. Public wireless connections pose significant security threats—they may be set up by hackers that pose as service providers, while really launching attacks on or monitoring the transmissions of unwitting users. The use of VPN software can make any passed-through packets unreadable. Contact your firm or school to find out how to set up VPN software.

In the Bank of America example above, the bank was burned. It couldn't verify that the lost tapes were encrypted, so it had to notify customers and incur the

17. Scrambling data using a code or formula, known as a cipher, such that it is hidden from those who do not have the unlocking key.

18. Code that unlocks encryption.

19. An attack that exhausts all possible password combinations in order to break into an account. The larger and more complicated a password or key, the longer a brute-force attack will take.

cost associated with assuming data had been breached.J. Mardesich, “Ensuring the Security of Stored Data,” CIO Strategy Center, 2009.

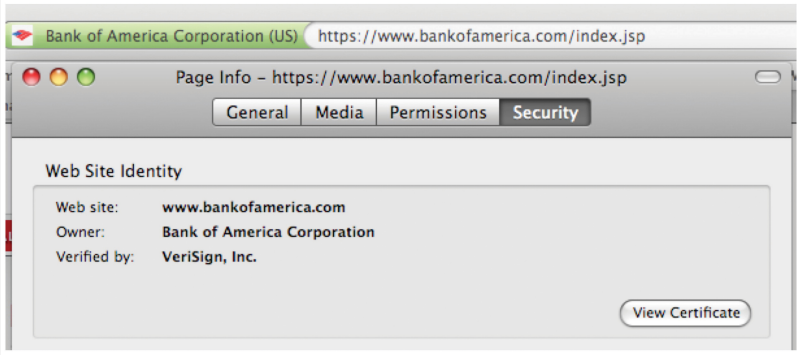
Encryption is not without its downsides. Key management is a potentially costly procedural challenge for most firms. If your keys aren’t secure, it’s the equivalent of leaving the keys to a safe out in public. Encryption also requires additional processing to scramble and descramble data—drawing more power and slowing computing tasks. Moore’s Law will speed things along, but it also puts more computing power in the hands of attackers. With hacking threats on the rise, expect to see laws and compliance requirements that mandate encrypted data, standardize encryption regimes, and simplify management.

How Do Web Sites Encrypt Transmissions?

Most Web sites that deal with financial transactions (e.g., banks, online stores) secure transmissions using a method called **public key encryption**[20]. The system works with two keys—a public key and a private key. The public key can "lock" or encrypt data, but it can't unlock it: that can only be performed by the private key. So a Web site that wants you to transmit secure information will send you a public key—you use this to lock the data, and no one that intercepts that transmission can break in unless they've got the private key. If the Web site does its job, it will keep the private key out of reach of all potentially prying eyes.

Wondering if a Web site's transmissions are encrypted? Look at the Web address. If it begins with "https" instead of "http", it should be secure. Also, look for the padlock icon in the corner of your Web browser to be closed (locked). Finally, you can double click the padlock to bring up a verification of the Web site's identity (verified by a trusted third party firm, known as a **certificate authority**[21]). If this matches your URL and indicates the firm you're doing business with, then you can be pretty sure verified encryption is being used by the firm that you intend to do business with.

Figure 13.6



In this screenshot, a Firefox browser is visiting Bank of America. The padlock icon was clicked to bring up digital certificate information. Note how the Web site's name matches the URL. The verifying certificate authority is the firm VeriSign.

20. A two key system used for securing electronic transmissions. One key distributed publicly is used to encrypt (lock) data, but it cannot unlock data. Unlocking can only be performed with the private key. The private key also cannot be reverse engineered from the public key. By distributing public keys, but keeping the private key, Internet services can ensure transmissions to their site are secure.
21. A trusted third party that provides authentication services in public key encryption schemes.

KEY TAKEAWAYS

- An organization's information assets are vulnerable to attack from several points of weakness, including users and administrators, its hardware and software, its networking systems, and various physical threats.
- Social engineering attempts to trick or con individuals into providing information, while phishing techniques are cons conducted through technology.
- While dangerous, a number of tools and techniques can be used to identify phishing scams, limiting their likelihood of success.
- Social media sites may assist hackers in crafting phishing or social engineering threats, provide information to password crackers, and act as conduits for unwanted dissemination of proprietary information.
- Most users employ inefficient and insecure password systems; however, techniques were offered to improve one's individual password regime.
- Viruses, worms, and Trojans are types of infecting malware. Other types of malware might spy on users, enlist the use of computing assets for committing crimes, steal assets, destroy property, serve unwanted ads, and more.
- Examples of attacks and scams launched through advertising on legitimate Web pages highlight the need for end-user caution, as well as for firms to ensure the integrity of their participating online partners.
- SQL injection and related techniques show the perils of poor programming. Software developers must design for security from the start—considering potential security weaknesses, and methods that improve end-user security (e.g., in areas such as installation and configuration).
- Encryption can render a firm's data assets unreadable, even if copied or stolen. While potentially complex to administer and resource intensive, encryption is a critical tool for securing an organization's electronic assets.

QUESTIONS AND EXERCISES

1. Consider your own personal password regime and correct any weaknesses. Share any additional password management tips and techniques with your class.
2. Why is it a bad idea to use variants of existing passwords when registering for new Web sites?
3. Relate an example of social engineering that you've experienced or heard of. How might the victim have avoided being compromised?
4. Have you ever seen phishing exploits? Have you fallen for one? Why did you take the bait, or what alerted you to the scam? How can you identify phishing scams?
5. Have you or has anyone you know fallen victim to malware? Relate the experience—how do you suppose it happened? What damage was done? What, if anything, could be done to recover from the situation?
6. Why are social media sites such a threat to information security? Give various potential scenarios where social media use might create personal or organizational security compromises.
7. Some users regularly update their passwords by adding a number (say month or year) to their code. Why is this bad practice?
8. What kind of features should a programmer build into systems in order to design for security? Think about the products that you use. Are there products that you feel did a good job of ensuring security during setup? Are there products you use that have demonstrated bad security design? How?
9. Why are SQL injection attacks more difficult to address than the latest virus threat?
10. How should individuals and firms leverage encryption?
11. Investigate how you might use a VPN if traveling with your laptop. Be prepared to share your findings with your class and your instructor.

13.4 Taking Action

LEARNING OBJECTIVES

1. Identify critical steps to improve your individual and organizational information security.
2. Be a tips, tricks, and techniques advocate, helping make your friends, family, colleagues, and organization more secure.
3. Recognize the major information security issues that organizations face, as well as the resources, methods, and approaches that can help make firms more secure.

Taking Action as a User

The weakest link in security is often a careless user, so don't make yourself an easy mark. Once you get a sense of threats, you understand the kinds of precautions you need to take. Security considerations then become more common sense than high tech. Here's a brief list of major issues to consider:

- *Surf smart.* Think before you click—question links, enclosures, download request, and the integrity of Web sites that you visit. Avoid suspicious e-mail attachments and Internet downloads. Be on guard for phishing, and other attempts to con you into letting in malware. Verify anything that looks suspicious before acting. Avoid using public machines (libraries, coffee shops) when accessing sites that contain your financial data or other confidential information.
- *Stay vigilant.* Social engineering con artists and rogue insiders are out there. An appropriate level of questioning applies not only to computer use, but also to personal interactions, be it in person, on the phone, or electronically.
- *Stay updated.* Turn on software update features for your operating system and any application you use (browsers, applications, plug-ins, and applets), and manually check for updates when needed. Malware toolkits specifically scan for older, vulnerable systems, so working with updated programs that address prior concerns lowers your vulnerable attack surface.
- *Stay armed.* Install a full suite of security software. Many vendors offer a combination of products that provide antivirus software that blocks infection, personal firewalls that repel unwanted intrusion, malware scanners that seek out bad code that might already be nesting on your

PC, antiphishing software that identifies if you're visiting questionable Web sites, and more. Such tools are increasingly being built into operating systems, browsers, and are deployed at the ISP or service provider (e-mail firm, social network) level. But every consumer should make it a priority to understand the state of the art for personal protection. In the way that you regularly balance your investment portfolio to account for economic shifts, or take your car in for an oil change to keep it in top running condition, make it a priority to periodically scan the major trade press or end-user computing sites for reviews and commentary on the latest tools and techniques for protecting yourself (and your firm).

- *Be settings smart.* Don't turn on risky settings like unrestricted folder sharing that may act as an invitation for hackers to drop off malware payloads. Secure home networks with password protection and a firewall. Encrypt hard drives—especially on laptops or other devices that might be lost or stolen. Register mobile devices for location identification or remote wiping. Don't click the "Remember me" or "Save password" settings on public machines, or any device that might be shared or accessed by others. Similarly, if your machine might be used by others, turn off browser settings that auto-fill fields with prior entries—otherwise you make it easy for someone to use that machine to track your entries and impersonate you. And when using public hotspots, be sure to turn on your VPN software to encrypt transmission and hide from network eavesdroppers.
- *Be password savvy.* Change the default password on any new products that you install. Update your passwords regularly. Using guidelines outlined earlier, choose passwords that are tough to guess, but easy for you (and only you) to remember. Federate your passwords so that you're not using the same access codes for your most secure sites. Never save passwords in nonsecured files, e-mail, or written down in easily accessed locations.
- *Be disposal smart.* Shred personal documents. Wipe hard drives with an industrial strength software tool before recycling, donating, or throwing away—remember in many cases "deleted" files can still be recovered. Destroy media such as CDs and DVDs that may contain sensitive information. Erase USB drives when they are no longer needed.
- *Back up.* The most likely threat to your data doesn't come from hackers; it comes from hardware failure.C. Taylor, "The Tech Catastrophe You're Ignoring," *Fortune*, October 26, 2009. Yet most users still don't regularly back up their systems. This is another do-it-now priority. Cheap, plug-in hard drives work with most modern operating systems to provide continual backups, allowing for quick rollback to earlier versions if you've accidentally ruined some vital work. And services

like EMC's Mozy provide monthly, unlimited backup over the Internet for less than what you probably spent on your last lunch (a fire, theft, or similar event could also result in the loss of any backups stored on-site, but Internet backup services can provide off-site storage and access if disaster strikes).
- *Check with your administrator.* All organizations that help you connect to the Internet—your ISP, firm, or school—should have security pages. Many provide free security software tools. Use them as resources. Remember—it's in their interest to keep you safe, too!

Taking Action as an Organization

Frameworks, Standards, and Compliance

Developing organizational security is a daunting task. You're in an arms race with adversaries that are tenacious and constantly on the lookout for new exploits. Fortunately, no firm is starting from scratch—others have gone before you and many have worked together to create published best practices.

There are several frameworks, but perhaps the best known of these efforts comes from the International Organization for Standards (ISO), and is broadly referred to as ISO27k or the ISO 27000 series. According to ISO.org, this evolving set of standards provides "a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System."

Firms may also face compliance requirements—legal or professionally binding steps that must be taken. Failure to do so could result in fine, sanction, and other punitive measures. At the federal level, examples include HIPAA (the Health Insurance Portability and Accountability Act), which regulates health data; the Graham-Leach-Bliley Act, which regulates financial data; and the Children's Online Privacy Protection Act, which regulates data collection on minors. U.S. government agencies must also comply with FISMA (the Federal Information Security Management Act), and there are several initiatives at the other government levels. By 2009, some level of state data breach laws had been passed by over thirty states, while multinationals face a growing number of statues throughout the world. Your legal team and trade associations can help you understand your domestic and international obligations. Fortunately, there are often frameworks and guidelines to assist in compliance. For example, the ISO standards include subsets targeted at the telecommunications and health care industries, and major credit card firms have created the PCI (payment card industry) standards. And there are skilled consulting professionals who can help bring firms up to speed in these areas, and help expand their organizational radar as new issues develop.

> Here is a word of warning on frameworks and standards: compliance does not equal security. Outsourcing portions security efforts without a complete, organizational commitment to being secure can also be dangerous. Some organizations simply approach compliance as a necessary evil: a sort of checklist that can reduce the likelihood of a lawsuit or other punitive measure.M. Davis, "What Will It Take?" *InformationWeek*, November 23, 2009. While you want to make sure you're doing everything in your power not to get sued, this isn't the goal. The goal is taking all appropriate measures to ensure that your firm is secure for your customers, employees, shareholders, and others. Frameworks help shape your thinking and expose things you should do, but security doesn't stop there—this is a constant, evolving process that needs to pervade the organization from the CEO suite and board, down to front line workers and potentially out to customers and partners. And be aware of the security issues associated with any mergers and acquisitions. Bringing in new firms, employees, technologies, and procedures means reassessing the security environment for all players involved.

The Heartland Breach

On inauguration day 2009, credit card processor Heartland announced that it had experienced what was one of the largest security breaches in history. The Princeton, New Jersey, based firm was, at the time, the nation's fifth largest payments processor. Its business was responsible for handling the transfer of funds and information between retailers and cardholders' financial institutions. That means infiltrating Heartland was like breaking into Fort Knox.

It's been estimated that as many as 100 million cards issued by more than 650 financial services companies may have been compromised during the Heartland breach. Said the firm's CEO, this was "the worst thing that can happen to a payments company and it happened to us."R. King, "Lessons from the Data Breach at Heartland," *BusinessWeek*, July 6, 2009. Wall Street noticed. The firm's stock tanked—within a month, its market capitalization had plummeted over 75 percent, dropping over half a billion dollars in value.T. Claburn, "Payment Card Industry Gets Encryption Religion," *InformationWeek*, November 13, 2009.

The Heartland case provides a cautionary warning against thinking that security ends with compliance. Heartland had in fact passed multiple audits, including one conducted the month before the infiltration began. Still, at least thirteen pieces of malware were uncovered on the firm's servers. Compliance does not equal security. Heartland was complaint, but a firm can be compliant and not be secure. Compliance is not the goal, security is.

Since the breach, the firm's executives have championed industry efforts to expand security practices, including encrypting card information at the point it is swiped and keeping it secure through settlement. Such "cradle-to-grave" encryption can help create an environment where even compromised networking equipment or intercepting relay systems wouldn't be able to grab codes.T. Claburn, "Payment Card Industry Gets Encryption Religion," *InformationWeek*, November 13, 2009; R. King, "Lessons from the Data Breach at Heartland," *BusinessWeek*, July 6, 2009. Recognize that security is a continual process, it is never done, and firms need to pursue security with tenacity and commitment.

Education, Audit, and Enforcement

Security is as much about people, process, and policy, as it is about technology.

From a people perspective, the security function requires multiple levels of expertise. Operations employees are involved in the day-to-day monitoring of existing systems. A group's R&D function is involved in understanding emerging threats and reviewing, selecting, and implementing updated security techniques. A team must also work on broader governance issues. These efforts should include representatives from specialized security and broader technology and infrastructure functions. It should also include representatives from general counsel, audit, public relations, and human resources. What this means is that even if you're a nontechnical staffer, you may be brought in to help a firm deal with security issues.

Processes and policies will include education and awareness—this is also everyone's business. As the Vice President of Product Development at security firm Symantec puts it, "We do products really well, but the next step is education. We can't keep the Internet safe with antivirus software alone."D. Goldman, "Cybercrime: A Secret Underground Economy," *CNNMoney*, September 17, 2009. Companies should approach information security as a part of their "collective corporate responsibility...regardless of whether regulation requires them to do so."Knowledge@Wharton, "Information Security: Why Cybercriminals Are Smiling," August 19, 2009.

For a lesson in how important education is, look no further than the head of the CIA. Former U.S. Director of Intelligence John Deutch engaged in shockingly loose behavior with digital secrets, including keeping a daily journal of classified information—some 1,000+ pages—on memory cards he'd transport in his shirt pocket. He also downloaded and stored Pentagon information, including details of covert operations, at home on computers that his family used for routine Internet access.N. Lewis, "Investigation Of Ex-Chief Of the C.I.A. Is Broadened," *New York Times*, September 17, 2000.

Employees need to know a firm's policies, be regularly trained, and understand that they will face strict penalties if they fail to meet their obligations. Policies without eyes (audit) and teeth (enforcement) won't be taken seriously. Audits include real-time monitoring of usage (e.g., who's accessing what, from where, how, and why; sound the alarm if an anomaly is detected), announced audits, and surprise spot checks. This function might also stage white hat demonstration attacks—attempts to hunt for and expose weaknesses, hopefully before hackers find them. Frameworks offer guidelines on auditing, but a recent survey found most organizations don't document enforcement procedures in their information security policies, that more than one-third do not audit or monitor user compliance with security policies, and that only 48 percent annually measure and review the effectiveness of security policies.A. Matwyshyn, *Harboring Data: Information Security, Law, and The Corporation* (Palo Alto, CA: Stanford University Press, 2009).

A firm's technology development and deployment processes must also integrate with the security team to ensure that from the start, applications, databases, and other systems are implemented with security in mind. The team will have specialized skills and monitor the latest threats and are able to advise on precautions necessary to be sure systems aren't compromised during installation, development, testing, and deployment.

What Needs to Be Protected and How Much Is Enough?

A worldwide study by PricewaterhouseCoopers and *Chief Security Officer* magazine revealed that most firms don't even know what they need to protect. Only 33 percent of executives responded that their organizations kept accurate inventory of the locations and jurisdictions where data was stored, and only 24 percent kept inventory of all third parties using their customer data.A. Matwyshyn, *Harboring Data: Information Security, Law, and The Corporation* (Palo Alto, CA: Stanford University Press, 2009). What this means is that most firms don't even have an accurate read on where their valuables are kept, let alone how to protect them.

So information security should start with an inventory-style auditing and risk assessment. Technologies map back to specific business risks. What do we need to protect? What are we afraid might happen? And how do we protect it? Security is an economic problem, involving attack likelihood, costs, and prevention benefits. These are complex trade-offs that must consider losses from theft or resources, systems damage, data loss, disclosure of proprietary information, recovery, downtime, stock price declines, legal fees, government and compliance penalties, and intangibles such as damaged firm reputation, loss of customer and partner confidence, industry damage, promotion of adversary, and encouragement of future attacks.

While many firms skimp on security, firms also don't want to misspend, targeting exploits that aren't likely, while underinvesting in easily prevented methods to thwart common infiltration techniques. Hacker conventions like DefCon can show some really wild exploits. But it's up to the firm to assess how vulnerable it is to these various risks. The local donut shop has far different needs than a military installation, law enforcement agency, financial institution, or firm housing other high-value electronic assets. A skilled risk assessment team will consider these vulnerabilities and what sort of countermeasure investments should take place.

Economic decisions usually drive hacker behavior, too. While in some cases attacks are based on vendetta or personal reasons, in most cases exploit economics largely boils down to

Adversary ROI = Asset value to adversary – Adversary cost.

An adversary's costs include not only the resources, knowledge, and technology required for the exploit, but also the risk of getting caught. Make things tough to get at, and lobbying for legislation that imposes severe penalties on crooks can help raise adversary costs and lower your likelihood of becoming a victim.

Technology's Role

Technical solutions often involve industrial strength variants of the previously discussed issues individuals can employ, so your awareness is already high. Additionally, an organization's approach will often leverage multiple layers of protection and incorporate a wide variety of protective measures.

Patch. Firms must be especially vigilant to pay attention to security bulletins and install software updates that plug existing holes, (often referred to as *patches*). Firms that don't plug known problems will be vulnerable to trivial and automated attacks. Unfortunately, many firms aren't updating all components of their systems with consistent attention. With operating systems automating security update installations, hackers have moved on to application targets. But a major study recently found that organizations took at least twice as long to patch application vulnerabilities as they take to patch operating system holes.S. Wildstrom, "Massive Study of Net Vulnerabilities: They're Not Where You Think They Are," *BusinessWeek*, September 14, 2009. And remember, software isn't limited to conventional PCs and servers. Embedded systems abound, and connected, yet unpatched devices are vulnerable. Malware has infected everything from unprotected ATM machinesP. Lilly, "Hackers Targeting Windows XP-Based ATM Machines," *Maximum PC*, June 4, 2009. to restaurant point-of-sale systemsR. McMillan, "Restaurants Sue Vendors after Point-of-Sale Hack," *CIO*, December 1, 2009. to fighter plane navigation systems.C. Matyszczyk, "French Planes Grounded by Windows Worm," *CNET*, February 8, 2009.

As an example of unpatched vulnerabilities, consider the DNS cache poisoning exploit described earlier in this chapter. The discovery of this weakness was one of the biggest security stories the year it was discovered, and security experts saw this as a major threat. Teams of programmers worldwide raced to provide fixes for the most widely used versions of DNS software. Yet several months after patches were available, roughly one quarter of all DNS servers were still unpatched and exposed.IBM, *X-Force Threat Report: 2008 Year in Review*, January 2009.

To be fair, not all firms delay patches out of negligence. Some organizations have legitimate concerns about testing whether the patch will break their system or

whether the new technology contains a change that will cause problems down the road.For example, the DNS security patch mentioned was incompatible with the firewall software deployed at some firms. And there have been cases where patches themselves have caused problems. Finally, many software updates require that systems be taken down. Firms may have uptime requirements that make immediate patching difficult. But ultimately, unpatched systems are an open door for infiltration.

Lock down hardware. Firms range widely in the security regimes used to govern purchase through disposal system use. While some large firms such as Kraft are allowing employees to select their own hardware (Mac or PC, desktop or notebook, iPhone or BlackBerry),N. Wingfield, "It's a Free Country...So Why Can't I Pick the Technology I Use in the Office?" *Wall Street Journal*, November 15, 2009. others issue standard systems that prevent all unapproved software installation and force file saving to hardened, backed-up, scanned, and monitored servers. Firms in especially sensitive industries such as financial services may regularly reimage the hard drive of end-user PCs, completely replacing all the bits on a user's hard drive with a pristine, current version—effectively wiping out malware that might have previously sneaked onto a user's PC. Other lock-down methods might disable the boot capability of removable media (a common method for spreading viruses via inserted discs or USBs), prevent Wi-Fi use or require VPN encryption before allowing any network transmissions, and more. The cloud helps here, too. (See Chapter 10 "Software in Flux: Partly Cloudy and Sometimes Free".) Employers can also require workers to run all of their corporate applications inside a remote desktop where the actual executing hardware and software is elsewhere (likely hosted as a virtual machine session on the organization's servers), and the user is simply served an image of what is executing remotely. This seals the virtual PC off in a way that can be thoroughly monitored, updated, backed up, and locked down by the firm.

In the case of Kraft, executives worried that the firm's previously restrictive technology policies prevented employees from staying in step with trends. Employees opting into the system must sign an agreement promising they'll follow mandated security procedures. Still, financial services firms, law offices, health care providers, and others may need to maintain stricter control, for legal and industry compliance reasons.

Lock down the network. Network monitoring is a critical part of security, and a host of technical tools can help.

22. A system that acts as a control for network traffic, blocking unauthorized traffic while permitting acceptable use.

Firms employ **firewalls**[22] to examine traffic as it enters and leaves the network, potentially blocking certain types of access, while permitting approved

communication. **Intrusion detection systems**[23] specifically look for unauthorized behavior, sounding the alarm and potentially taking action if something seems amiss. Some firms deploy **honeypots**[24]—bogus offerings meant to distract attackers. If attackers take honeypot bait, firms may gain an opportunity to recognize the hacker's exploits, identify the IP address of intrusion, and take action to block further attacks and alert authorities.

Many firms also deploy **blacklists**[25]—denying the entry or exit of specific IP addresses, products, Internet domains, and other communication restrictions. While blacklists block known bad guys, **whitelists**[26] are even more restrictive—permitting communication only with approved entities or in an approved manner.

These technologies can be applied to network technology, specific applications, screening for certain kinds of apps, malware signatures, and hunting for anomalous patterns. The latter is important, as recent malware has become polymorphic, meaning different versions are created and deployed in a way that their signature, a sort of electronic fingerprint often used to recognize malicious code, is slightly altered. This also helps with zero-day exploits, and in situations where whitelisted Web sites themselves become compromised.

Many technical solutions, ranging from network monitoring and response to e-mail screening, are migrating to "the cloud." This can be a good thing—if network monitoring software immediately shares news of a certain type of attack, defenses might be pushed out to all clients of a firm (the more users, the "smarter" the system can potentially become—again we see the power of network effects in action).

Lock down partners. Insist partner firms are compliant, and audit them to ensure this is the case. This includes technology providers and contract firms, as well as value chain participants such as suppliers and distributors. Anyone who touches your network is a potential point of weakness. Many firms will build security expectations and commitments into performance guarantees known as service level agreements (SLAs).

Lock down systems. Audit for SQL injection and other application exploits. The security team must constantly scan exploits and then probe its systems to see if it's susceptible, advising and enforcing action if problems are uncovered. This kind of auditing should occur with all of a firm's partners.

23. A system that monitors network use for potential hacking attempts. Such a system may take preventative action to block, isolate, or identify attempted infiltration, and raise further alarms to warn security personnel.

24. A seemingly tempting, but bogus target meant to draw hacking attempts. By monitoring infiltration attempts against a honeypot, organizations may gain insight into the identity of hackers and their techniques, and they can share this with partners and law enforcement.

25. Programs that deny the entry or exit of specific IP addresses, products, Internet domains, and other communication restrictions.

26. Highly restrictive programs that permit communication only with approved entities and/or in an approved manner.

Access controls can also compartmentalize data access on a need-to-know basis. Such tools can not only enforce access privileges, they can help create and monitor audit trails to help verify that systems are not being accessed by the unauthorized, or in suspicious ways.

Audit trails are used for deterring, identifying, and investigating these cases. Recording, monitoring, and auditing access allows firms to hunt for patterns of abuse. Logs can detail who, when, and from where assets are accessed. Giveaways of nefarious activity may include access from unfamiliar IP addresses, from nonstandard times, accesses that occur at higher than usual volumes, and so on. Automated alerts can put an account on hold or call in a response team for further observation of the anomaly.

Single-sign-on tools can help firms offer employees one very strong password that works across applications, is changed frequently (or managed via hardware cards or mobile phone log-in), and can be altered by password management staff.

Multiple administrators should jointly control key systems. Major configuration changes might require approval of multiple staffers, as well as the automatic notification of concerned personnel. And firms should employ a recovery mechanism to regain control in the event that key administrators are incapacitated or uncooperative. This balances security needs with an ability to respond in the event of a crisis. Such a system was not in place in the earlier described case of the rogue IT staffer who held the city of San Francisco's networks hostage by refusing to give up vital passwords.

Have failure and recovery plans. While firms work to prevent infiltration attempts, they should also have provisions in place that plan for the worst. If a compromise has taken place, what needs to be done? Do stolen assets need to be devalued (e.g., accounts terminated, new accounts issued)? What should be done to notify customers and partners, educate them, and advise them through any necessary responses? Who should work with law enforcement and with the media? Do off-site backups or redundant systems need to be activated? Can systems be reliably restored without risking further damage?

Best practices are beginning to emerge. While postevent triage is beyond the scope of our introduction, the good news is that firms are now sharing data on breaches. Given the potential negative consequences of a breach, organizations once rarely admitted they'd been compromised. But now many are obligated to do so. And the broad awareness of infiltration both reduces organizational stigma in coming forward, and allows firms and technology providers to share knowledge on the techniques used by cybercrooks.

Information security is a complex, continually changing, and vitally important domain. The exploits covered in this chapter seem daunting, and new exploits constantly emerge. But your thinking on key issues should now be broader. Hopefully you've now embedded security thinking in your managerial DNA, and you are better prepared to be a savvy system user and a proactive participant working for your firm's security. Stay safe!

KEY TAKEAWAYS

- End users can engage in several steps to improve the information security of themselves and their organizations. These include surfing smart, staying vigilant, updating software and products, using a comprehensive security suite, managing settings and passwords responsibly, backing up, properly disposing of sensitive assets, and seeking education.
- Frameworks such as ISO27k can provide a road map to help organizations plan and implement an effective security regime.
- Many organizations are bound by security compliance commitments and will face fines and retribution if they fail to meet these commitments.
- The use of frameworks and being compliant is not equal to security. Security is a continued process that must be constantly addressed and deeply ingrained in an organization's culture.
- Security is about trade-offs—economic and intangible. Firms need to understand their assets and risks in order to best allocate resources and address needs.
- Information security is not simply a technical fix. Education, audit, and enforcement regarding firm policies are critical. The security team is broadly skilled and constantly working to identify and incorporate new technologies and methods into their organizations. Involvement and commitment is essential from the boardroom to frontline workers, and out to customers and partners.

QUESTIONS AND EXERCISES

1. Visit the security page for your ISP, school, or employer. What techniques do they advocate that we've discussed here? Are there any additional techniques mentioned and discussed? What additional provisions do they offer (tools, services) to help keep you informed and secure?
2. What sorts of security regimes are in use at your university, and at firms you've worked or interned for? If you don't have experience with this, ask a friend or relative for their professional experiences. Do you consider these measures to be too restrictive, too lax, or about right?
3. While we've discussed the risks in having security that is too lax, what risk does a firm run if its security mechanisms are especially strict? What might a firm give up? What are the consequences of strict end-user security provisions?
4. What risks does a firm face by leaving software unpatched? What risks does it face if it deploys patches as soon as they emerge? How should a firm reconcile these risks?
5. What methods do firms use to ensure the integrity of their software, their hardware, their networks, and their partners?
6. An organization's password management system represents "the keys to the city." Describe personnel issues that a firm should be concerned with regarding password administration. How might it address these concerns?