Chapter 5

CyberSecurity, Compliance, and Business Continuity

Learning Outcomes

1. Describe the types of cybercrimes facing organizations and critical infrastructures, explain the motives of cybercriminals, and evaluate the financial value of cybersecurity.
2. Explain both low-tech and high-tech methods used to gain access to a company's networks and databases, the vulnerabilities of information systems, and cybercrime symptoms. Describe the critical role of senior management, acceptable use policies, security procedures, and IT for defense-in-depth.
3. Describe types and characteristics of fraud, the role of corporate governance, and IT tools to detect fraudulent activities.
4. Explain general, administrative, and endpoint controls needed to secure information systems, networks, and wireless devices; and to manage risk.
5. Describe network security measures needed to protect the endpoints or wired and wireless networks and deny unauthenticated access.
6. Describe the role of the internal control environment in deterring fraud and complying with regulations.
7. Explain the benefits of business continuity and disaster recovery planning methods and why audits are an important part of control systems.

QUICK LOOK at Chapter 5, CyberSecurity, Compliance, and Business Continuity

Since 2010, damaging cyberattacks targeting classified and confidential information, trade secrets, and other intellectual property have worsened. Hacking or malware (short for *malicious software*) were linked to almost every data breach, and organized criminals were behind the majority of breaches. Cyberspies and criminals had robbed tens of billions of dollars' worth of data from U.S. companies each year. Hacktivists destroyed brand images and customer relationships and forced the shutdown of the CIA's (Central Intelligence Agency) web site. The always-on world was victimized by mobile malware and infected apps posted by cybercriminals on iTunes (in violation of their policy) to lure users into downloading rogue applications—which then spread from smartphones into corporate networks. U.S. officials reported that combating electronic espionage against corporate America by hackers in China and other countries is a matter of national and economic security.

As you read in this chapter, the mobile, social, connected infrastructures of this decade are more vulnerable to cyberattack. International, federal, and state laws and industry regulations mandate that organizations invest in cybersecurity defenses, audits, and internal controls to secure confidential data and defend against fraud and unauthorized transactions, such as money laundering. Inarguably, everyone needs to understand cybersecurity vulnerabilities, threats, exploits, and defenses.

CASE 1 OPENING CASE

Managing BYOD Security Risks

BYOD (bring your own device) means that employees are using many different types of personal devices to store and process enterprise data, and connect to enterprise networks.

People wanting to use their mobile devices at work has led to the practice of **bring your own device (BYOD)—**which is part of the **consumerization of information technology (COIT)** trend. The BYOD practice for smartphones is seeing enterprises take risks they would not consider taking for conventional computing devices (Dunn, 2012). Many smartphones are not being managed as secure devices, with fewer than one in five adding anti-malware and only half using data encryption.

Trying to Hold Back the BYOD Movement

Previously, employers provided employees with computers that were more advanced than personal ones—and not convenient to carry. Then Androids and iPhones, tablets, e-readers, and other mobile devices flipped that relationship. Figure 5.1 shows that the number of non-PC devices sold (425 million) had exceeded PC sales (390 million) in 2011.

Employees wanted to know "Why can't I use my devices at work?" Many expected instant approval and support for their new iPads within hours of its release. Actually BYOD

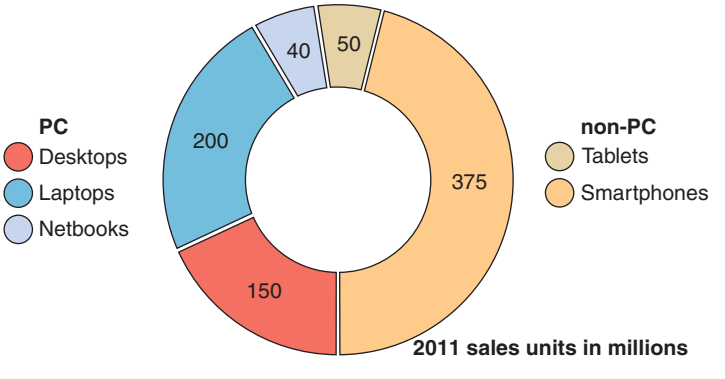


Figure 5.1 Number of units of PC and non-PC devices sold, in millions, in 2011.
Source: Deloitte, 2011.

raises several legitimate areas of concern. New vulnerabilities are created when personal and business data and communications are mixed together. Also, the mobile infrastructure may not be able to support the increase in mobile network traffic and data processing—causing unacceptable delays or requiring additional investments.

Gaining Control of the BYOD Megatrend

Forrester Research, Inc. estimated that 60 percent of companies had begun allowing BYOD by 2012. Chip-manufacturer Intel projects that 70 percent of its employees will use personal devices for some aspect of their job by 2014. No longer was it a question of whether to allow employees to use their own devices, but how to gain control over devices that employees were using at work. The four challenges that have to be resolved are device control costs, security threats, compliance, and privacy.

1. **Device control costs.** One potential benefit of BYOD is saving on costs associated with company-owned equipment. But these cost savings can be wiped out by increased IT costs—mostly for IT personnel who struggle to maintain control over new and existing mobile devices. Every personal device needs to be properly accounted for all as well as the apps they run. With the number of mobile apps hitting 1.3 million in mid-2012–compared to only 75,000 apps for PCs—managing employee-owned devices is more complex and expensive.
2. **Security threats.** Mobile devices and the networks they run can be cybersecurity landmines—capable of compromising confidential, sensitive, or classified data. A major security hole stems from the fact that the latest tablets, smartphones, and other handhelds often rely on unsecured wireless networks—and users don't use encryption or strong password controls. Consequences for data breaches or other compromises include damaged brand or reputation, lost customers, and multi-million-dollar fines.

   Data and ISs need to be protected from unauthorized access, including when an employee's device is lost or stolen, or an employee leaves the company. All **cybersecurity controls**—authentication, access control, data confidentiality, and intrusion detection—implemented on corporate-owned resources over the last decade can be rendered useless on an employee-owned device.
3. **Compliance.** Organizations are subject to national and international regulations and standards that specify how data can or cannot be collected and stored, as well as how it must be made available in the event of an audit or legal action. Companies need to insure and be able to prove that enterprise data stored on personal devices are in compliance, e.g., encrypted, password protected, unaltered, etc.
4. **Privacy.** Controls placed on employee-owned devices can infringe on personal privacy. For instance, organizations could know what sites were visited or movies were watched, what was done on sick days, what texts were sent/received, and all social media activities during work hours and off-hours.

Example of BYOD Solution: AT&T Toggle

It's inevitable that companies will invest in BYOD solutions, most likely from their mobile network or enterprise apps vendors. As is standard with cybersecurity investments, managers need to assess, select, and implement a BYOD solution that is aligned with their organization's IT governance plan. Because this is a new software market, there is no clear leader, and major changes are to be expected.

AT&T was the first U.S. carrier to announce a BYOD application. **AT&T Toggle** separates and safeguards business data on employees' mobile devices by creating two modes: personal and work as shown in Figure 5.2.

1. ***Personal mode:*** When not working, owners can text, watch videos, and play games on their mobile device as they otherwise would. Personal activities remain segregated and inaccessible to the organization.
2. ***Work mode*** (or container): While at work, employees switch to their work environment. In this mode, users can access corporate e-mail, applications, calendars and more, just as they would on company-provided computing resources.

Figure 5.2 AT&T Toggle is a BYOD app and service.

Access to business data is managed via a mobile device client installed on the employee's device. This client creates a **work container** that is a "walled off" area on the device where employees can access corporate content securely. All corporate data is fully encrypted and compliant with company policy. Company visibility is limited to the work container only. The company does not have access to the personal side. Employees keep control of that personal mode.

AT&T Toggle offers a web portal that IT administrators use to:

- Manage and monitor employee access to company resources.
- Add, update, and delete business applications on employees' personal devices.
- Wipe all corporate data stored in work mode if an employee leaves the company or loses the device.

The initial version of AT&T Toggle can be used on devices running Android 2.2 or higher, and with any service provider.

Discuss

1. Explain the pressures driving the BYOD trend.
2. Why had organizations initially rejected the idea?
3. What contributed to BYOD acceptance?
4. Identify and discuss four key challenges of BYOD.
5. How does AT&T Toggle attempt to resolve the challenges you identified in question #4?
6. With just a smartphone, users can conduct nearly all their banking business at any time. The level of flexibility and convenience opens up new avenues for fraud and cybercrime. To what extent are users willing to give up convenience for their own security? And for the security of their companies?

Decide

7. View the brief video titled "Learn More About AT&T Toggle." Find the link in the Chapter 5 Link Library on the book's web site, or visit *wireless.att.com* and search for the title *(wireless.att.com/businesscenter/popups/video/learn-more-about-toggle.jsp).*
   a. How is access to the work container protected? What determines the strength of this protection?
   b. Would you feel confident that your privacy was protected using Toggle?

Debate

8. How do you achieve the right balance to protect the enterprise's security and the employee's privacy? What is the right balance of security and privacy?

5.1 Up Close Look at Cybercrimes, Criminals, and Motivations

Critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

The U.S. has 18 critical infrastructure sectors. See Figure 5.3.

During the five months between October 2011 and February 2012, there were 86 reported attacks on computer systems in the U.S. that control national **critical infrastructure,** according to the Department of Homeland Security (DHS, dhs.gov/). Over the same period a year earlier, there had been only 11 such serious attacks. These infrastructure attacks did not cause significant damage, but the eightfold spike is alarming to DHS, Congress, and private sector. Congress reacted by working on legislation that requires stronger cybersecurity standards to defend against increasingly harmful cyberattacks.

Attacks on critical infrastructure could significantly disrupt the functioning of government and business—and trigger cascading effects far beyond the targeted sector and physical location of the incident (see Figure 5.3.)

New cybersecurity dangers are emerging and overtaking familiar threats—viruses, lost disks, and DoS attacks. Experts believe the greatest cybersecurity dangers in the next few years involve **persistent threats** (discussed in *IT at Work 5.1*), mobile computing, and the use of social media for **social engineering.** Social engineering tactics are used by hackers and corporate spies to trick people into revealing login information or access codes. Two social engineering methods are:

1. **Pretexting** is the use of a story that convinces someone into revealing secret information. For instance, a hacker uses readily available phone numbers and names to call a worker claiming to be the systems administrator who needs to reset passwords to protect the company from hacking. The hacker has the employee re-log into the network say everything he is typing to get the username and password.
2. **Baiting** is the use of an incentive to get a user to perform an insecure action. A common bait is to offer a free app or video for clicking a link in a text message and voting for best video game. Clicking the link downloads malware.

Many cyber threats and cybersecurity challenges that organizations face today were unimaginable 10 years ago, such as the BYOD issues discussed in the Opening Case #1. And longstanding threats such as of fraud and identity theft still remain. Cyber threats will continue to emerge, evolve, and worsen over the next 10 years and beyond. *IT at Work 5.1* provides an overview of results of the *2012 Global State of Information Security Survey.*

Figure 5.3 Six of the 18 national critical infrastructures (from upper-left, clockwise): commercial facilities; defense industrial base; transportation systems; national monuments and icons; banking and finance; and agriculture and food.
Photos courtesy of United States Department of Homeland Security.

Source: Homeland Security, "Critical Infrastructure Protection," *http://www.dhs.gov/files/programs/critical.shtm.*

IT at Work 5.1

Global State of Information Security Survey

The *2012 Global State of Information Security Survey* is conducted by the consulting firm PwC US *(PricewaterhouseCoopers. pwc.com)* and *CIO* and *CSO* magazines (PWC, 2012). According to this 9th annual survey of almost 10,000 security executives from 138 countries, only 72 percent of respondents were confident that their organization's information security defenses were effective. Confidence in their defenses' effectiveness had dropped significantly since 2006. Mark Lobel, a principal in PwC's Advisory practice, explained: "Companies now have greater insights than ever before into the landscape of cybercrime and other security events—and they're translating this information into security investments specifically focused on three areas: prevention, detection, and operational web technologies."

Advanced Persistent Threat (APT) Attacks

A significant percent of respondents across industries agreed that one of the most dangerous cyber threats is an **advanced persistent threat (APT) attack**. APT is a stealth network attack in which an unauthorized person gains access to a network and remains undetected for a long time. APTs are designed for long-term espionage. Skilled hackers launch APT attacks to steal data continuously (for example, daily) over months or years—rather than to cause damage that would reveal their presence. APT attacks target organizations with high-value information, such as national defense, manufacturing, and financial. APT threats are driving organizations' cybersecurity spending because only 16 percent are prepared to defend against them.

Cloud, mobile, and social expand exposure

Cloud computing has complicated cybersecurity. For 23 percent of organizations, cloud technologies have worsened their exposure primarily because they cannot enforce or verify their cloud providers' cybersecurity policies. In addition, mobile devices and social media expose organizations to new and significant threats.

Questions

1. What three areas are organizations focusing their infosec investments on?
2. Explain APT attacks.
3. What industries are at greatest risk of APT attacks? Why?
4. What is the largest perceived risk of cloud computing?

According to the 2012 Data Breach Investigations Report (DBIR), a global study of data theft at companies and government agencies, it takes a long time for victims to find out they have been hacked. In 2011, 92 percent of data breaches were discovered by a third party and not the company being breached. The Ponemon Institute (*ponemon.org*), an information security research firm, has found that a data breach typically costs an organization from $5 million to $8 million—from fines imposed by government agencies, legal fees, mandated improvements in defenses, and costs of notifying and compensating individuals whose data was exposed.

Why then are cyberattacks getting worse? Because networks are used by **hacktivists** (hacker-activists or *hacking for a cause*) looking for media attention; by hackers looking to steal **credentials** such as banking PINS and passwords; by industrial spies looking for trade secrets; by employees performing their jobs, or gaming or gambling online; and by customers buying products and services. The obvious problem is how to identify and block all malicious traffic while allowing legitimate traffic into a network. Such reliable precision and power may never exist.

Apps and other software have holes that hackers exploit—and users often do not know about unless they keep tabs on the latest cyber vulnerabilities. And these vulnerabilities appear almost daily.

TOP DOWN SECURITY

The 2012 Data Breach Investigations Report (DBIR, 2012) revealed that in most cases it is not IT that will keep users safe; rather it is a combination of management and best practices. The DBIR also revealed that 97 percent of data breaches evaluated in the study were avoidable and did not require hackers to possess special skills, resources, or customization. Approximately 30 percent of breaches impacting 84 percent of records breached were the result of stolen login credentials—usernames and passwords.

Complying with regulations is considered one of the primary business risks for highly-regulated industries such as energy utilities, health care, and financial firms. For example, the North American Electric Reliability Corporation (*NERC.com*) can fine a company up to $1 million a day for non-compliance (Chickowski, 2012). Large financial institutions have to comply with dozens of regulations by building information security programs with controls that are appropriate to protect the business and data.

HIGH-VISIBILITY CYBERCRIMINALS AND HACKTIVISTS

Advanced persistent threat (APT) attackers want to remain unnoticed so that they can continue to steal data, as described in *IT at Work 5.1*. Profit-motivated cybercriminals often operate in stealth mode. In contrast, hackers and hacktivists with personal agendas carry out high-profile attacks.

LulzSec is a hacker group and spin-off of the loosely organized hacking collective **Anonymous.** Lulz is slang that can be interpreted as *laugh (LOLs)*. They claimed responsibility for several high-profile attacks, including the compromise of user accounts from Sony Pictures in 2011. LulzSec does not appear to hack for financial profit. At times, they act as **hacktivists.**

Hacktivist is short for hacker-activists, or *hacking for a cause*.

Denial of service (DoS) is a type of attack where a web site or network is bombarded with traffic to make them crash.

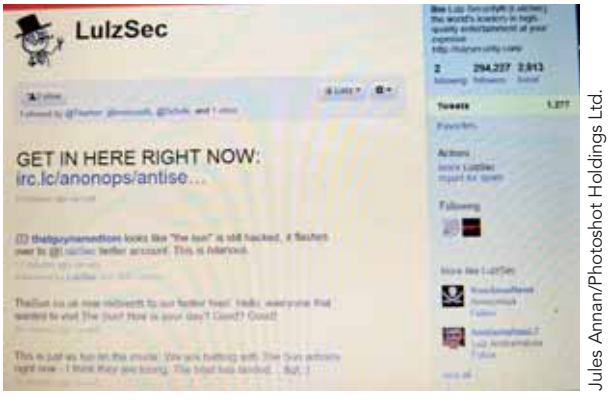
Hacktivists' Motivations and Dangerous Pranks.

These types of cybercriminals seemed to take on everyone from Sony and security firm RSA to the CIA (Central Intelligence Agency) and a Mexican drug cartel throughout 2011 and 2012. During the Arab Spring (Arab Revolutions), hacktivists **LulzSec** and **Anonymous** showed how vulnerable anyone's online presence was, even that of major governments. LulzSec and Anonymous even have logos, as shown in Figures 5.4 and 5.5. One of LulzSec's specialties is finding web sites with poor security, and then stealing and posting information from them online. Their attacks may seem more like Internet pranks than serious cyberwarfare, but they are still illegal**.**

Hacktivist Attacks and Victims.

Hackers committed daring data breaches, compromises, data leaks, thefts, threats, and privacy invasions in 2012. Here are several of those cases.

Combined Systems Inc. Proudly displaying its hacktivist flag (shown in Figure 5.5), Anonymous took credit for knocking Combined Systems Inc. offline and stealing



Jules Annan/Photoshot Holdings Ltd.

Figure 5.4 LulzSec.

REVELLIBEAUMONT/SIPA/Newscom

Figure 5.5 Anonymous is represented by a flag with imagery of the "suit without a head" to represent its leaderless organization and anonymity.

personal data from its clients. Anonymous went after Combined Systems, which sells tear gas and crowd-control devices to law enforcement and military organizations, to protest war profiteers.

CIA. In February 2012, for the second time in less than a year, Anonymous launched a denial of service (DoS) attack that forced the CIA web site offline. The CIA take-down followed a busy week for the hacktivists. Within 10 days, the group also went after Chinese electronics manufacturer Foxconn, American Nazi groups, anti-virus firm Symantec, and the office of Syria's president, which are described next.

Foxconn. Apple was facing worldwide scrutiny over questionable working conditions at Foxconn, a Chinese company that assembles iPhones, iPads, and devices for Dell, Sony, IBM, Microsoft, and others. Hacktivists SwaggSec took up the cause by stealing staff's e-mail logins and credentials.

American Nazi Party. To protest hate speech, Anonymous defaced and took down the American Nazi Party web site and white supremacist site, Whitehonor. The attacks were part of Anonymous' Operation Blitzkrieg campaign.

Symantec. Hacker YamaTough posted the source code to Symantec's pcAnywhere software used by customers to access remote PCs. The leak came when YamaTough's extortion attempt against Symantec failed.

Office of the Syrian President. Anonymous leaked e-mails from Syrian President Bashar Assad's office, including a candid e-mail in which one of Assad's media advisers prepped him for an interview with Barbara Walters and told him that the "American psyche can be easily manipulated."

Hamas. Israeli hacking group IDF Team (Israeli Defense Force) launched an attack against a Hamas web site knocking it offline to protest the site's anti-Israeli position. Israeli and Arab hackers battled for over a month. Saudi Arabian hacker 0xOmar posted 15,000 Israeli credit-card numbers. IDF Team retaliated by posting Arabs' credit-card credentials. After 0xOmar disrupted the Tel Aviv Stock Exchange, Israel's El Al Airlines, and two major Israeli banks, the IDF Team countered by hitting the Saudi Stock Exchange and Abu Dhabi Securities Exchange.

Scotland Yard and the FBI. Police had arrested several high-ranking Anonymous hackers, including Ryan Cleary, the British teenager charged with launching DoS attacks against British and U.S. targets. Anonymous intercepted and posted the audio of a 17-minute conference call in which the two agencies discussed plans to track down and prosecute Anonymous hackers.

OnGuardOnline. To protest the controversial Stop Online Piracy Act (SOPA), Anonymous took down OnGuardOnline.gov, the U.S. government's cybersecurity guidance web site. Anonymous defaced the site with a message threatening to destroy dozens of government and corporate web sites if SOPA was passed.

STEALTH, PROFIT-MOTIVATED CYBERCRIMES

Most hack activities do not become headline-grabbers until after the incidents are detected and reported. However, victimized companies are reluctant to discuss them, so statistics are scarce. Most data breaches go unreported, according to cybersecurity experts, because corporate victims fear that disclosure would damage their stock price, or because they never knew they were hacked in the first place.

Theft of Trade Secrets and Other Confidential Information. Theft of trade secrets has always been a threat from corporate moles, disgruntled employees, and other insiders. Of course, now it is easier to steal information remotely, mostly because of smartphones and the BYOD trend. Hackers' preferred *modus operandi* is to break into employees' mobile devices and leapfrog into employers' networks—stealing secrets without a trace.

U.S. cybersecurity experts and government officials are increasingly concerned about breaches from other countries into corporate networks, either through mobile devices or by other means. Mike McConnell, a former director of national intelligence, warned: "In looking at computer systems of consequence—in government, Congress, at the Department of Defense, aerospace, companies with valuable trade secrets—we've not examined one yet that has not been infected by an advanced persistent threat." In the meantime, companies are leaking critical information, often without realizing it. Scott Aken, a former FBI agent who specialized in counterintelligence and computer intrusion. "In most cases, companies don't realize they've been burned until years later when a foreign competitor puts out their very same product — only they're making it 30 percent cheaper."

Do-Not-Carry Rules. Now, U.S. companies and government agencies are imposing **do-not-carry rules**, which are based on the assumption that devices will inevitably be compromised," according to Mike Rogers, chairman of the House Intelligence Committee. Members could bring only "clean" devices and are forbidden from connecting to the government's network while abroad. Rogers said he travels "electronically naked" to insure cybersecurity during and after a trip. *IT at Work 5.2* describes the reasons following do-not-carry rules.

The types and scope of cyberthefts and other profit-motivated attacks are illustrated by the following incidents.

U.S. Chamber of Commerce and Member Organizations Hacked. The U.S. Chamber of Commerce is headquartered in Washington, D.C. (Figure 5.6). The Chamber did not learn that it and its member organizations were the victims of a cybertheft for months until the FBI informed them that servers in China were stealing data from four of their Asia policy experts, who travel to Asia frequently (Perloth, 2011). It's possible that the experts' mobile devices had been infected with malware that was transmitting information and files back to the hackers. By the time the Chamber hardened (secured) its network, hackers had stolen at least six weeks of e-mails, most of which were with the largest U.S. corporations. Even later, the Chamber learned that its office printer and a thermostat in one of its corporate apartments were communicating with an Internet address in China. The Chamber did not disclose how hackers had infiltrated its systems, but its first step after the attack was to implement do-not-carry rules.

IT at Work 5.2

Traveling Electronically-Clean

When Kenneth G. Lieberthal, an expert at the Brookings Institution, travels to other countries, he follows a routine that seems straight from a secret agent movie. He leaves his smartphone and laptop at home. Instead he brings loaner devices, which he erases before he leaves the U.S. and wipes clean the minute he returns. While traveling, he disables Bluetooth and Wi-Fi and never lets his phone out of his sight. While in meetings, he not only turns off his phone, but also removes the battery for fear his microphone could be turned on remotely.

Lieberthal connects to the Internet only through an encrypted, password-protected channel. He never types in a password directly, but copies and pastes his password from a USB thumb drive. By not typing his password, he eliminates the risk of having it stolen if key-logging software got installed on his device.

Questions

1. Many travelers might consider Lieberthal's method too inconvenient. Clearly, his electronically clean methods are time consuming and expensive. In your opinion, is there a tradeoff between cybersecurity and convenience? Explain.
2. Create a list of best cybersecurity practices for travelers based on Lieberthal's methods.

Figure 5.6 The United States Chamber of Commerce was hacked over several months.

Hackers Put Hijacked Web Views Up for Sale for Web Fraud. In a new twist on web site exploits for profit, web hackers have begun to turn sites they have exploited (infected with malware) into sources of fraudulent web traffic for anyone willing to pay. The hackers use inline frames (iframes) injected into the HTML code of a web site to redirect visitors from the legitimate site to anywhere on the Web. According to RSA's security blog, the site is operated by a Russia-based group of hackers who created the capability for their own use first. They then realized its potential profitability as a larger service to others who want to profit from web advertising fraud, launch drive-by download attacks on users' browsers, or run other scams based on illegitimately gained page views.

Tech Note 5.1

iframes load and execute web pages within the body of another page. Legitimate web sites use iframes to redirect to content while concealing its source. iframes are widely used in various Facebook apps to deliver content within the Facebook environment. But they're also used by marginally ethical search engine optimization hackers, and are a standard element of most web fraud.

Sony. Sony suffered over a dozen data breaches in 2011 stemming from attacks that compromised over 100 million customer records and gained access to their passwords. Sony-owned web sites were hacked including Sony PlayStation Network (PSN), Sony Online Entertainment (SOE), and Sony Pictures. The hacker attack on its PSN cost the company about $170 million. On the PlayStation (PS3) menu, Sony highlighted a system update option with news of the PS3 software hack, as shown in Figure 5.7. According to a notice posted on the SOE web site (*soe.com/securityupdate/*) on May 2, 2011, Sony temporarily suspended all online multiplayer SOE games "until we could verify their security."

Sony reported that there was no evidence that their main credit card database was compromised, which is in a completely separate and secured environment. However, Sony's customers who reuse their passwords were at risk from attackers using the stolen password data to access their accounts on other sites. Sony faced ongoing customer relations fallout and class-action lawsuits for failing to protect confidential information.

OBJECTIVES OF CYBERSECURITY

As these hacker, hacktivist, and intrusion examples indicate, cybersecurity is a never-ending process of insuring the availability and integrity of data and other computing resources for legitimate users and uses; and defending against threats to

Figure 5.7 A Sony PS3 menu highlighting the system update option with recent news stories of users hacking into the PS3 software.

data, information systems, networks, privacy, commerce, national security, financial stability, and more.

Cybersecurity needs to accomplish the following:

- Make data and documents available and accessible 24/7 while simultaneously restricting access
- Implement and enforce procedures and acceptable use policies (AUPs) for data, networks, hardware, and software that are company-owned or employee-owned as discussed in the opening case
- Promote secure and legal sharing of information among authorized persons and partners
- Insure compliance with government regulations and laws
- Prevent attacks by having network intrusion defenses in place
- Detect, diagnose, and respond to incidents and attacks in real time
- Maintain internal controls to prevent unauthorized alteration of data and records
- Recover from business disasters and disruptions quickly

Business policies, procedures, training, and disaster recovery plans as well as hardware and software technologies play critical roles in cybersecurity.

Questions

1. Define national critical infrastructure. Give three examples.
2. Why are cyberattacks on critical infrastructure particularly dangerous?
3. Explain why hackers and corporate spies use social engineering.
4. Explain why advanced persistent threat (APT) attacks are one of the most dangerous cyber threats.
5. What are the motives of LulzSec and Anonymous?
6. Why do most data breaches go unreported?
7. Why are government agencies and organizations imposing do-not-carry rules?

5.2 IS Vulnerabilities and Threats

Every enterprise has data, files, communications, and business records that profit-motivated criminals (who may be across the globe or be trusted employees) want. Those risks can stem from insiders, outsiders, criminal organizations, or malware. **Malware** are viruses, worms, trojan horses, spyware, and any other type of disruptive, destructive, or unwanted programs. Threats range from high-tech exploits to gain access to a company's networks and databases to non-tech tactics to steal laptops and whatever is available. Because security terms, such as *threats* and *exploits*, have precise meanings, the key terms and their meanings are listed in Table 5.1.

TABLE 5.1 Cybersecurity Terms

Term	Definition
Threat	Something or someone that may result in harm to an asset
Risk	Probability of a threat exploiting a vulnerability
Vulnerability	A weakness that threatens the confidentiality, integrity, or availability (CIA) of an asset
CIA triad (confidentiality, integrity, availability)	Three key cybersecurity principles
Exploit	Tool or technique that takes advantage of a vulnerability
Risk management	Process of identifying, assessing, and reducing risk to an acceptable level
Exposure	Estimated cost, loss, or damage that can result if a threat exploits a vulnerability
Access control	Security feature designed to restrict who has access to a network, IS, or data.
Audit	The process of generating, recording, and reviewing a chronological record of system events to determine their accuracy
Encryption	Transforming data into scrambled code to protect it from being understood by unauthorized users
Plaintext or clear-text	Readable text
Ciphertext	Encrypted text
Authentication	Method (usually based on username and password) by which an IS validates or verifies that a user is really who he or she claims to be
Biometrics	Methods to identify a person based on a biological feature, such as a fingerprint or retina
Firewall	Software or hardware device that controls access to a private network from a public network (Internet) by analyzing data packets entering or exiting it
Intrusion detection system (IDS)	A defense tool used to monitor network traffic (packets) and provide alerts when there is suspicious traffic, or to quarantine suspicious traffic
Fault tolerance	The ability of an IS to continue to operate when a failure occurs, but usually for a limited time or at a reduced level
Botnet (short for Bot network)	A network of hijacked computers that are controlled remotely—typically to launch spam or spyware. Also called software robots. Botnets are linked to a range of malicious activity, including identity theft and spam.

VULNERABILITIES

Vulnerabilities are weaknesses that threaten the confidentiality, integrity, or availability (CIA) of an asset.

- **Confidentiality** is the avoidance of the unauthorized disclosure of information. Confidentiality involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content.
- **Integrity** is the property that data or files have not been altered in an unauthorized way.
- **Availability** is the property that data is accessible and modifiable when needed by those authorized to do so.

Passwords. The function of a password together with a username is to **authenticate** a user's identity to verify that the person has the right to access a computer or network. Weak passwords create vulnerabilities. Passwords that are shared or not kept secret are useless. Unfortunately, too many people are lazy or unaware of the dangers and choose passwords that are easily guessable, short, common, or a word in the dictionary. Their disregard for this security measure makes it easy for hackers to break into many accounts simply by trying common passwords such as "password," "12345678," "qwerty" or "abc123." Strong passwords contain a combination of upper- and lower-case letters, numbers, and punctuation marks, and at least eight characters long although ten characters is better.

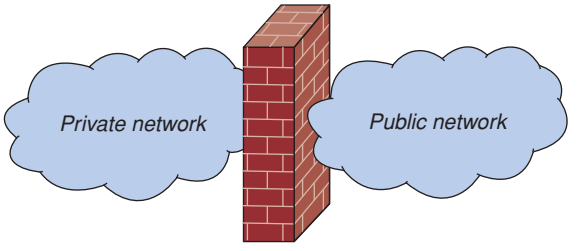


Figure 5.8 Firewalls create barriers to separate insecure public networks from private networks.

Internal Threats. Threats from employees, referred to as **internal threats,** are a major challenge largely due to the many ways an employee can carry out malicious activity. Insiders may be able to bypass physical security (e.g., locked doors) and technical security (e.g., passwords) measures that organizations have in place to prevent unauthorized access. Why? Because technology defenses such as firewalls, intrusion detection systems (IDS), and locked doors mostly protect against external threats.

A **firewall** is an integrated collection of security measures designed to prevent unauthorized access. A network firewall is similar to firewalls in buildings that are designed to isolate one network from another, as shown in Figure 5.8. To protect private networks and devices from external cyberthreats, a firewall inspects incoming or outgoing traffic—allowing in legitimate traffic and denying suspicious traffic. If a hacker learns an employee's password, the firewall offers no defense because the hacker would be using legitimate credentials.

IDS are sensors or tools that monitor traffic on a network after it has passed through the firewall. An IDS is designed to detect a number of threats, including:

- An attacker who is using the identity or credentials of a legitimate user to gain access to an IS, device, or network
- A legitimate user who performs actions he is not authorized to do
- A user who tries to disguise or cover up his actions by deleting audit files or system logs.

Cloud Computing and Social Network Risks. Social networks and cloud computing increase vulnerabilities by providing a single point of failure and attack. Critical, sensitive, and private information is at risk, and like previous IT trends, such as wireless networks, the goal is connectivity, often with little concern for security. As social networks increase their services, the gap between services and cybersecurity also increases. E-mail viruses and malware have been declining for years as e-mail security has improved. This trend continues as communication shifts to social networks and newer smartphones. Unfortunately, malware finds its way to users through security vulnerabilities in these new services and devices. Web filtering, user education, and strict policies are necessary to help prevent widespread outbreaks.

In Twitter and Facebook, users invite in and build relationships with others. Cybercriminals hack into these trusted relationships using stolen log-ins. Fake antivirus and other attacks that take advantage of user trust are very difficult to detect.

An overriding reason why these networks and services increase exposure to risk is the **time-to-exploitation** of today's sophisticated spyware and mobile viruses. Time-to-exploitation is the elapsed time between when vulnerability is discovered and when it's exploited. That time has shrunk from months to minutes so IT staff have

ever-shorter timeframes to find and fix flaws before being compromised by an attack. Some attacks exist for as little as two hours, which means that enterprise IT security systems must have real-time protection.

When new vulnerabilities are found in operating systems, applications, or wired and wireless networks, patches are released by the vendor or security organization. **Patches** are software programs that users download and install to fix the vulnerability. Microsoft, for example, releases patches that it calls **service packs** to update and fix vulnerabilities in its operating systems, including Vista, and applications, including Office 2010. Service packs are made available at Microsoft's web site.

Left undetected or unprotected, vulnerabilities provide an open door for IT attacks and business disruptions and their financial damages. Despite even the best technology defenses, infosec incidents will occur mostly because of users who do not follow secure computing practices and procedures.

Phishing and Web-Based Threats. Companies increasingly adopt external, web-based applications, and employees bring consumer applications into the enterprise. Criminal enterprises are following the money on the Internet where that have a global market of potential victims.

Phishing is a deceptive method of stealing confidential information by pretending to be a legitimate organization, such as PayPal, a bank, credit card company, or other trusted source. Phishing messages include a link to a fraudulent phish web site that looks like the real one. When the user clicks the link to the phish site, he or she is asked for a credit card number, social security number, account number, or password. Phishing remains successful and profitable for criminals.

Criminals use the Internet and private networks to hijack large numbers of PCs to spy on users, spam them, shake down businesses, and steal identities. But why are they so successful? The Information Security Forum (*securityforum.org*), a self-help organization that includes many Fortune 100 companies, compiled a list of the top information problems and discovered that 9 of the top 10 incidents were the result of 3 factors:

1. Mistakes or human error
2. Malfunctioning systems
3. Misunderstanding the effects of adding incompatible software to an existing system

Unfortunately, these factors can too easily defeat cybersecurity technologies that companies and individuals use to protect their information. A fourth factor identified by the Security Forum is motivation, as described in *IT at Work 5.3*.

IT at Work 5.3

Money Laundering, Organized Crime, and Terrorist Financing

According to the U.S. Department of State (*state.gov*), organized crime rings rely on money laundering to fund their operations. This practice poses international and national security threats. It undermines free enterprise by crowding out the private sector, and it threatens the financial stability of nations.

Funds used to finance terrorist operations are very difficult to track. Despite this obscurity, by adapting methods used to combat money laundering, such as financial analysis and investigations, authorities can significantly disrupt the financial networks of terrorists and build a paper trail and base of evidence to identify and locate leaders of terrorist organizations and cells.

International organized crime syndicates, al-Qaeda groups, and other cybercriminals steal hundreds of billions of dollars every year. Cybercrime is safer and easier than selling drugs, dealing in black market diamonds, or robbing banks. Online gambling offers easy fronts for international money-laundering operations.

GOVERNMENT REGULATIONS

IT defenses must satisfy ever-stricter government and international regulations. Primary regulations are the Sarbanes–Oxley Act (SOX), Gramm-Leach-Bliley Act (GLB), Federal Information Security Management Act (FISMA), and USA Patriot Act in the U.S. Canada's Personal Information Protection and Electronic Document Act (PIPEDA); and Basel III (global financial services) all mandate the protection of personally identifiable information (PII). The director of the Federal Trade Commission (FTC) bureau of consumer protection warned that the agency would bring enforcement action against small businesses lacking adequate policies and procedures to protect consumer data.

Two accepted models for IT governance are **enterprise risk management (ERM)** and **COBIT (Control Objectives for Information and Related Technology).** ERM is a risk-based approach to managing an enterprise that integrates internal control, the Sarbanes–Oxley Act mandates, and strategic planning. ERM is intended to be part of routine planning processes rather than a separate initiative. The ideal place to start is with buy-in and commitment from the board and senior leadership COBIT, which is described in *IT at Work 5.4*, is an internationally accepted IT governance and control framework for aligning IT with business objectives, delivering value, and managing associated risks. It provides a reference for management, users, and IS audit, control, and security practitioners.

INDUSTRY STANDARDS

Industry groups imposed their own standards to protect their customers and their members' brand images and revenues. One example is the **Payment Card Industry Data Security Standard (PCI DSS)** created by Visa, MasterCard, American Express, and Discover.

PCI is required for all members, merchants, or service providers that store, process, or transmit cardholder data. PCI DSS mandates that retailers ensure that Web-facing applications are protected against known attacks by applying either of the following two methods:

1. Have all custom application code reviewed for vulnerabilities by an application security firm.
2. Install an application layer firewall in front of Web-facing applications. Each application will have its own firewall to protect against intrusions and malware.

IT at Work 5.4

COBIT and IT Governance Best Practices

IT governance is the supervision, monitoring, and control of the organization's IT assets. The IT Governance Institute (*itgi.org*) publishes Control Objectives for Information and Related Technology (COBIT), which many companies use as their IT governance guide. COBIT can be downloaded from isaca.org.

The Sarbanes–Oxley Act requires that companies provide proof that their financial applications and systems are controlled (secured) to verify that financial reports can be trusted. This requires that IT security managers work with business managers to do a risk assessment to identify which systems depend on technical controls rather than on business process controls. To meet COBIT, IT systems should be based on the following three principles:

Principle of economic use of resources: This principle acknowledges that the cost of infosec needs to be balanced with its benefits. It's the basic cost/benefit principle that you're familiar with. For example, you wouldn't spend more to protect your auto, home, or other asset than they are worth. Because it's possible, for instance, for companies to set a very low value on the confidential data of customers and employers and therefore avoid basic infosec defenses, the next two principles try to make sure that doesn't happen.

Principle of legality: This principle requires that companies invest in infosec to meet minimum legal requirements. This is a basic security principle, just like having hand railings on stairways, fire extinguishers, and alarm systems.

Accounting principles: These principles require that the integrity, availability, and reliability of data and information systems be maintained.

The purpose of the PCI DSS is to improve customers' trust in e-commerce, especially when it comes to online payments, and to increase the web security of online merchants. To motivate following these standards, the penalties for noncompliance are severe. The card brands can fine the retailer, and increase transaction fees for each credit or debit card transaction. A finding of noncompliance can be the basis for lawsuits.

CompTIA Infosec Survey. In its 2012 information security survey, the Computing Technology Industry Association (CompTIA, *comptia.org*), reported that only 22 percent of organizations have a formal policy in place governing use of mobile devices at work. The online survey of 500 business and IT professionals from various industries found that 70 percent of IT staff believed that security considerations are the greatest risk involved in supporting mobility.

The respondents identified a number of security risks from mobile devices: downloading unauthorized apps (48 percent), lost or stolen devices (42 percent), mobile-specific viruses and malware (41 percent), open Wi-Fi networks (41 percent), USB flash drives (40 percent), and personal use of business devices (40 percent).

The survey found that tablets are the top mobile device choice for purchase in the next year. Currently, smartphones are used at more organizations than standard cell phones; 84 percent of respondents use their smartphones for light work, such as e-mail or web browsing, while tablets are used for note taking, giving presentations, and as a communications device.

Organizations have to balance business objectives and security objectives, which may not always be in synch.

DEFENSE-IN-DEPTH MODEL

Defense-in-depth is a multi-layered approach to infosec. The basic principle is that when one defense layer fails, another layer provides protection. For example, if a wireless network's security was compromised, then having encrypted data would still protect the data provided that the thieves could not decrypt it.

The success of any type of IT project depends on the commitment and involvement of executive management, also referred to as the "tone at the top." The same is true of IT security. When senior management shows its commitment to IT security, it becomes important to others too. This infosec *tone* makes users aware that insecure practices and mistakes will not be tolerated. Therefore, an IT security and internal control model begins with senior management commitment and support, as shown in Figure 5.9. The model views infosec as a combination of people, processes, and technology.

Step 1: Senior management commitment and support. Senior managers' influence is needed to implement and maintain security, ethical standards, privacy practices, and internal control. The Committee of Sponsoring Organizations of the Treadway Commission (COSO, *coso.org/key.htm*) defines **internal control** as a *process* designed to provide *reasonable* assurance of effective operations and reliable financial reporting. Internal control is discussed later in this chapter.

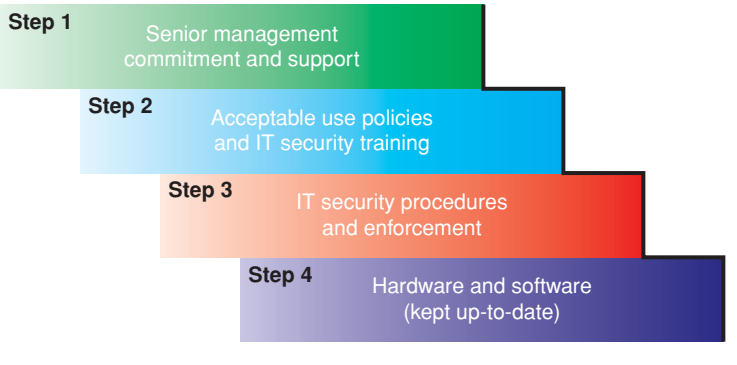


Figure 5.9 Cybersecurity defense-in-depth model.

Step 2: Acceptable use policies and IT security training. The next step in building an effective IT security program is to develop security policies and provide training to ensure that everyone is aware of and understands them. The greater the understanding of how security affects production levels, customer and supplier relationships, revenue streams, and management's liability, the more security will be incorporated into business projects and proposals.

Most critical is an **acceptable use policy (AUP)** that informs users of their responsibilities. An AUP is needed for two reasons: (1) to prevent misuse of information and computer resources; and (2) to reduce exposure to fines, sanctions, and legal liability. To be effective, the AUP needs to define users' responsibilities, acceptable and unacceptable actions, and consequences of noncompliance. E-mail, Internet, and computer AUPs should be thought of as an extension of other corporate policies, such as those that address physical safety, equal opportunity, harassment, and discrimination.

Step 3: IT Security Procedures and Enforcement. If users' activities are not monitored for compliance, the AUP is useless. Therefore, the next step is to implement monitoring procedures, training, and enforcement of the AUP. Businesses cannot afford the infinite cost of perfect security, so they calculate the proper level of protection. The calculation is based on the digital assets' risk exposure. The risk exposure model for digital assets is comprised of the five factors shown in Table 5.2.

Another risk assessment method is the **business impact analysis (BIA)**. BIA is an exercise that determines the impact of losing the support or availability of a resource. For example, for most people, the loss of a smartphone would have greater impact than loss of a digital camera. BIA helps identify the minimum resources needed to recover, and prioritizes the recovery of processes and supporting systems. A BIA needs to be updated as new threats to IT emerge. After the risk exposure of digital assets has been estimated, then informed decisions about investments in infosec can be made.

Step 4: Hardware and Software. The last step in the model is implementation of software and hardware needed to support and enforce the AUP and secure practices.

Keep in mind that security is an ongoing unending process, and not a problem that can be solved with hardware or software. Hardware and software security defenses cannot protect against irresponsible business practices.

One of the biggest mistakes managers make is underestimating IT vulnerabilities and threats. Most workers use their laptops and mobiles for both work and leisure, and in an era of multitasking, they often do both at the same time. Yet off-time or off-site use of devices remains risky because, despite policies, employees continue to engage in dangerous online and communication habits. Those habits make them a weak link in an organization's otherwise solid security efforts. These threats can be classified as *unintentional* or *intentional*.

TABLE 5.2 Risk Exposure Model for Digital Assets

Factor	Cost and Operational Considerations
1. Asset's value to the company	What are the costs of replacement, recovery, or restoration? What is the recoverability time?
2. Attractiveness of the asset to a criminal	What is the asset's value (on a scale of low to high) to identity thieves, industrial spies, terrorists, or fraudsters?
3. Legal liability attached to the asset's loss or theft	What are the potential legal costs, fines, and restitution expenses?
4. Operational, marketing, and financial consequences	What are the costs of business disruption, delivery delays, lost customers, negative media attention, inability to process payments or payroll, or a drop in stock prices?
5. Likelihood of a successful attack against the asset	Given existing and emerging threats, what is the probability the asset will be stolen or compromised?

UNINTENTIONAL THREATS

Unintentional threats fall into three major categories: human errors, environmental hazards, and computer system failures.

1. **Human errors** can occur in the design of the hardware or information system. They can also occur during programming, testing, or data entry. Not changing default passwords on a firewall or failing to manage patches create security holes. Human errors also include untrained or unaware users responding to phishing or ignoring security procedures. Human errors contribute to the majority of internal control and infosec problems.
2. **Environmental hazards** include volcanoes, earthquakes, blizzards, floods, power failures or strong fluctuations, fires (the most common hazard), defective air conditioning, explosions, radioactive fallout, and water-cooling-system failures. In addition to the primary damage, computer resources can be damaged by side effects, such as smoke and water. Such hazards may disrupt normal computer operations and result in long waiting periods and exorbitant costs while computer programs and data files are recreated.
3. **Computer systems failures** can occur as the result of poor manufacturing, defective materials, and outdated or poorly maintained networks (recall the network crash at LAX airport in Chapter 4). Unintentional malfunctions can also happen for other reasons, ranging from lack of experience to inadequate testing.

INTENTIONAL THREATS

Examples of intentional threats include theft of data; inappropriate use of data (e.g., manipulating inputs); theft of mainframe computer time; theft of equipment and/or programs; deliberate manipulation in handling, entering, processing, transferring, or programming data; labor strikes, riots, or sabotage; malicious damage to computer resources; destruction from viruses and similar attacks; and miscellaneous computer abuses and Internet fraud.

Botnets. A **botnet** is a collection of bots (computers infected by software robots). Those infected computers, called **zombies**, can be controlled and organized into a network of zombies on the command of a remote botmaster (also called bot herder). Botnets expose infected computers, as well as other network computers, to the following threats:

- **Spyware:** Zombies can be commanded to monitor and steal personal or financial data.
- **Adware:** Zombies can be ordered to download and display advertisements. Some zombies even force an infected system's browser to visit a specific web site.
- **Spam:** Most junk e-mail is sent by zombies. Owners of infected computers are usually blissfully unaware that their machines are being used to commit a crime.
- **Phishing:** Zombies can seek out weak servers that are suitable for hosting a phishing web site, which looks like a legitimate web site, to trick the users into inputting confidential data.

Botnets are extremely dangerous because they scan for and compromise other computers, and then can be used for every type of crime and attack against computers, servers, and networks.

Questions

1. Explain confidentiality, integrity, and availability.
2. What is the purpose of passwords, firewalls, and intrusion-detection systems (IDS)?
3. Give an example of a weak and a strong password.
4. What is time-to-exploitation?
5. What is a service pack?
6. Explain phishing.
7. Why is money laundering a national security threat?
8. What is an acceptable use policy (AUP)?
9. Why do companies need an enforced AUP?
10. Define and give two examples of an unintentional threat.
11. Define and give two examples of an intentional threat.
12. Define botnet and explain its risk.

5.3 Defending Against Fraud

According to the 2011 LexisNexis True Cost of Fraud Study, retail merchants incur over a $100 billion in fraud losses due to unauthorized transactions, fees, and interest linked to chargebacks (funds returned to the credit card company)—almost 10 times the amount incurred by banks (LexisNexis, 2011). These losses are only customer-related—and do not include fraud committed by employees or in other industries. The number of fraudulent transactions decreased between 2010 and 2011, but average dollar value of a completed fraudulent transaction is increasing. Challenges for U.S. merchants who ship internationally include delay in payment confirmation, verification of customer identity, limited jurisdiction, and ability to reclaim merchandise and costs.

Crimes fall into two categories depending on the tactics of the criminal: violent and nonviolent. Fraud is a nonviolent crime because instead of a gun or knife, fraudsters use deception, confidence, and trickery—all are types of social engineering. Fraudsters carry out their crimes by abusing the power of their position or by taking advantage of the trust, ignorance, or laziness of others.

INSIDER FRAUD

Insider fraud is a term referring to a variety of criminal behaviors perpetrated by an organization's own employees or contractors. Other terms for this crime are *internal, employment,* or *occupational* fraud. **Internal fraud** refers to the deliberate misuse of the assets of one's employer for personal gain. Internal audits and internal controls are essential to the prevention and detection of occupation frauds. Several examples are listed in Table 5.3.

Experts estimate that on average it costs companies 3 percent to 5 percent of revenue each year (ACFE, 2012). When profit margins are thin, internal fraud can put companies out of business. The truth is that companies often are unaware of all the frauds committed within their company.

INTERNAL FRAUD PREVENTION AND DETECTION

The single-most-effective fraud prevention technique is the perception of detection and punishment. If a company shows its employees that it can find out everything that every employee does and will prosecute to the fullest extent anyone who commits fraud, then the feeling that "I can get away with it" drops drastically. The Catch-22 is that companies may have limited resources that hinder a proper fraud diagnosis or forensic accounting investigation, even though they cannot afford unrecoverable losses either.

TABLE 5.3 Types and Characteristics of Organizational Fraud

Type of Fraud	Does This Fraud Impact Financial Statements?	Typical Characteristics
Operating management corruption	No	Occurs *off the books.* Median loss due to corruption: over 6 times greater than median loss due to misappropriation ($530,000 vs. $80,000)
Conflict of interest	No	A breach of confidentiality, such as revealing competitors' bids, often occurs with bribery
Bribery	No	Uses positional power or money to influence others
Embezzlement or misappropriation	Yes	Employee theft: employees' access to company property creates the opportunity for embezzlement
Senior management financial reporting fraud	Yes	Involves a massive breach of trust and leveraging of positional power
Accounting cycle fraud	Yes	This fraud is called "earnings management" or earning engineering, which are in violation of GAAP (Generally Accepted Accounting Principles) and all other accounting practices. See *aicpa.org*

Corporate Governance. IT has a key role to play in demonstrating effective corporate governance in order to prevent fraud. Regulators look favorably on companies that can demonstrate good corporate governance and best practice operational risk management. Management and staff of such companies will then spend less time worrying about regulations and more time adding value to their brand and business.

Internal fraud prevention measures are based on the same controls used to prevent external intrusions—perimeter defense technologies, such as firewalls, e-mail scanners, and biometric access. They are also based on human resource (HR) procedures, such as recruitment screening and training.

Intelligent Analysis, Audit Trails, and Anomaly Detection. Much of this detection activity can be handled by intelligent analysis engines using advanced data warehousing and analytics techniques. These systems take in audit trails from key systems and personnel records from the HR and finance departments. The data are stored in a data warehouse where they are analyzed to detect anomalous patterns, such as excessive hours worked, deviations in patterns of behavior, copying huge amounts of data, attempts to override controls, unusual transactions, and inadequate documentation about a transaction. Information from investigations is fed back into the detection system so that it learns. Since insiders might work in collusion with organized criminals, insider profiling is important to find wider patterns of criminal networks.

Identity Theft. One of the worst and most prevalent crimes is identity theft. Such thefts where individuals' Social Security and credit card numbers are stolen and used by thieves are not new. Criminals have always obtained information about other people—by stealing wallets or dumpster digging. But widespread electronic sharing and databases have made the crime worse. Because financial institutions, data processing firms, and retail businesses are reluctant to reveal incidents in which their customers' personal financial information may have been stolen, lost, or compromised, laws continue to be passed that force those notifications.

Questions

1. Define fraud and insider occupational fraud.
2. How can internal fraud be prevented?
3. How can internal fraud be detected?
4. Explain why data on laptops and computers should be encrypted.
5. Explain how identity theft can occur.

5.4 Information Assurance and Risk Management

The objective of IT security management practices is to defend all of the components of an information system, specifically data, software applications, hardware, and networks. Before they make any decisions concerning defenses, people responsible for security must understand the requirements and operations of the business, which form the basis for a customized defense strategy. In the next section, we describe the major defense strategies.

DEFENSE STRATEGY

The defense strategy and controls that should be used depend on what needs to be protected and the cost-benefit analysis. That is, companies should neither under-invest nor over-invest. The SEC and FTC impose huge fines for data breaches to deter companies from under-investing in data protection. The following are the major objectives of defense strategies:

1. Prevention and deterrence. Properly designed controls may prevent errors from occurring, deter criminals from attacking the system, and, better yet, deny access to unauthorized people. These are the most desirable controls.

2. Detection. Like a fire, the earlier an attack is detected, the easier it is to combat, and the less damage is done. Detection can be performed in many cases by using special diagnostic software, at a minimal cost.

3. Contain the damage. This objective is to minimize or limit losses once a malfunction has occurred. This process is also called *damage control*. This can be accomplished, for example, by including a **fault-tolerant system** that permits operation in a degraded mode until full recovery is made. If a fault-tolerant system does not exist, a quick and possibly expensive recovery must take place. Users want their systems back in operation as fast as possible.

4. Recovery. A recovery plan explains how to fix a damaged information system as quickly as possible. Replacing rather than repairing components is one route to fast recovery.

5. Correction. Correcting the causes of damaged systems can prevent the problem from occurring again.

6. Awareness and compliance. All organization members must be educated about the hazards and must comply with the security rules and regulations.

A defense strategy is also going to require several controls, as shown in Figure 5.10. **General controls** are established to protect the system regardless of the specific application. For example, protecting hardware and controlling access to the data center are independent of the specific application. **Application controls** are safeguards that are intended to protect specific applications.

GENERAL CONTROLS

The major categories of general controls are physical controls, access controls, data security controls, communication network controls, and administrative controls.

Physical Controls. Physical security refers to the protection of computer facilities and resources. This includes protecting physical property such as computers, data centers, software, manuals, and networks. It provides protection against most natural hazards as well as against some human hazards. Appropriate physical security may include several controls such as the following:

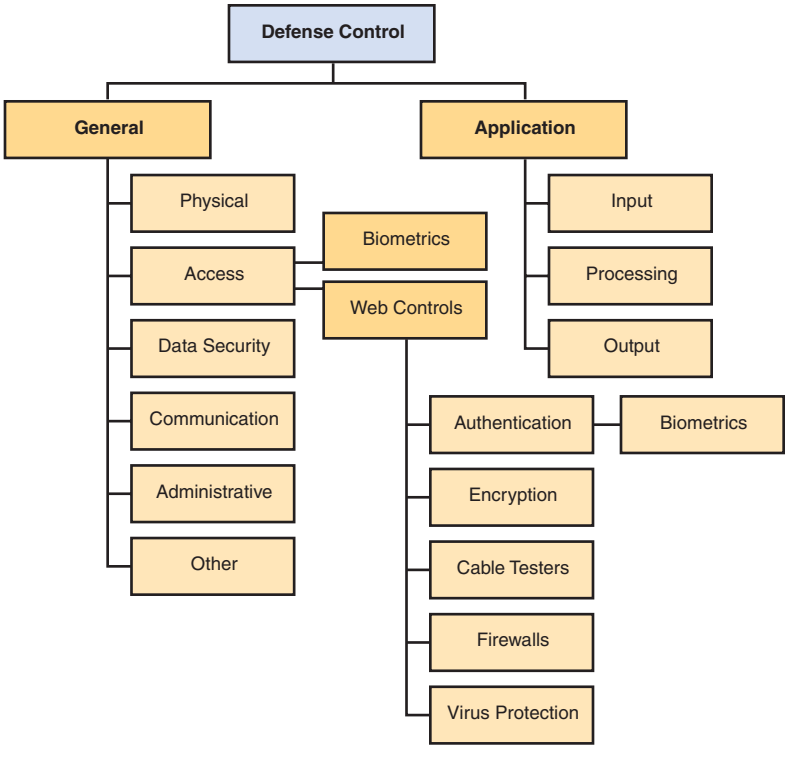


Figure 5.10 Major defense controls.

- Appropriate design of the data center. For example, the data center should be noncombustible and waterproof.
- Shielding against electromagnetic fields
- Good fire prevention, detection, and extinguishing systems, including sprinkler systems, water pumps, and adequate drainage facilities
- Emergency power shutoff and backup batteries, which must be maintained in operational condition
- Properly designed and maintained air-conditioning systems
- Motion-detector alarms that detect physical intrusion

Access Controls. Access control is the management of who is and is not authorized to use a company's hardware and software. Access control methods, such as firewalls and access control lists, restrict access to a network, database, file, or data. It is the major defense line against unauthorized insiders as well as outsiders. Access control involves authorization (having the right to access) and authentication, which is also called user identification (proving that the user is who he claims to be).

Authentication methods include:

- Something only the user knows, such as a password
- Something only the user has, for example, a smart card or a token
- Something only the user is, such as a signature, voice, fingerprint, or retinal (eye) scan; implemented via biometric controls, which can be physical or behavioral

Biometric Controls. A **biometric control** is an automated method of verifying the identity of a person, based on physical or behavioral characteristics. For example, fingerprint scanners are used for identification, as shown in Figure 5.11.

Most biometric systems match some personal characteristic against a stored profile. The most common biometrics are:

- **Thumbprint or fingerprint.** Each time a user wants access, a thumbprint or fingerprint (finger scan) is matched against a template containing the authorized person's fingerprint to identify him or her.
- **Retinal scan.** A match is attempted between the pattern of the blood vessels in the back-of-the-eye retina that is being scanned and a prestored picture of the retina.

Biometric controls are now integrated into many e-business hardware and software products. Biometric controls do have some limitations: they are not accurate in certain cases, and some people see them as an invasion of privacy.

Administrative Controls. While the previously discussed general controls are technical in nature, administrative controls deal with issuing guidelines and monitoring compliance with the guidelines. Examples of such controls are shown in Table 5.4.

UPPA/Photoshot Holdings Ltd.

Figure 5.11 Biometric scanner.
Source: Department of Homeland Security, *http://www.dhs.gov/files/programs/usv.shtm*.

TABLE 5.4 Administrative Controls

- Appropriately selecting, training, and supervising employees, especially in accounting and information systems
- Fostering company loyalty
- Immediately revoking access privileges of dismissed, resigned, or transferred employees
- Requiring periodic modification of access controls (such as passwords)
- Developing programming and documentation standards (to make auditing easier and to use the standards as guides for employees)
- Insisting on security bonds or malfeasance insurance for key employees
- Instituting separation of duties, namely, dividing sensitive computer duties among as many employees as economically feasible in order to decrease the chance of intentional or unintentional damage
- Holding periodic random audits of the system

Endpoint Security and Control. Many managers underestimate business risk posed by unencrypted portable storage devices—which are examples of *endpoints*. Business data is often carried on thumb drives, smartphones, and removable memory cards without IT's permission, oversight, or sufficient protection against loss or theft. Handhelds and portable storage devices put sensitive data at risk. According to the market research firm Applied Research-West, three out of four workers save corporate data on thumb drives. According to their study, 25 percent save customer records, 17 percent store financial data, and 15 percent store business plans on thumb drives, but less than 50 percent of businesses routinely encrypt those drives and even less consistently secure data copied onto smartphones.

Portable devices that store confidential customer or financial data must be protected no matter who owns them—employees or the company. If there are no security measures to protect handhelds or other mobile/portable storage, data must not be stored on them because it exposes the company to liability, lawsuits, and fines. For smaller companies, a single data breach could bankrupt the company.

Questions

1. What are the major objectives of a defense strategy?
2. What are general controls?
3. Define access control.
4. What are biometric controls? Give two examples.
5. What is endpoint security?

5.5 Network Security

As a defense, companies need to implement network access control (NAC) products. NAC tools are different from traditional security technologies and practices that focus on file access. While file-level security is useful for protecting data, it does not keep unauthorized users out of the network in the first place. NAC technology, on the other hand, helps businesses lock down their networks against criminals.

Network security measures involve three types of defenses, which are referred to as *layers*.

1. **First layer: Perimeter security** to control access to the network. Examples are antivirus software and firewalls.
2. **Second layer: Authentication** to verify the identity of the person requesting access to the network. Examples are usernames and passwords.
3. **Third layer: Authorization** to control what authenticated users can do once they are given access to the network. Examples are permissions and directories.

Details of these three defense layers are shown in Figure 5.12.

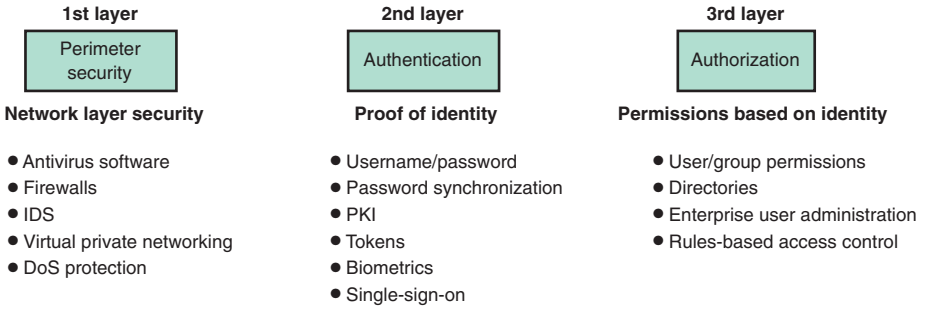


Figure 5.12 Three layers of network security measures.

PERIMETER SECURITY AND FIREWALLS

The major objective of perimeter security is access control. The technologies used to protect against malware (e.g., firewalls, IDS, and IDP) also protect the perimeter. A firewall enforces an access-control policy between two networks. Firewalls need to be configured to enforce the company's security procedures and policies. A network has several firewalls, but they still cannot stop all malware. See Figure 5.13. For example, each virus has a signature, which identifies it. Firewalls and antivirus software that have been updated—and know of that virus' signature—can block it. But viruses pass through a firewall if the firewall cannot identify it as a virus. For example, a newly released virus whose signature has not yet been identified or that is hidden in an e-mail attachment could be allowed into the network. That's the reason why firewalls and antivirus software require continuous updating.

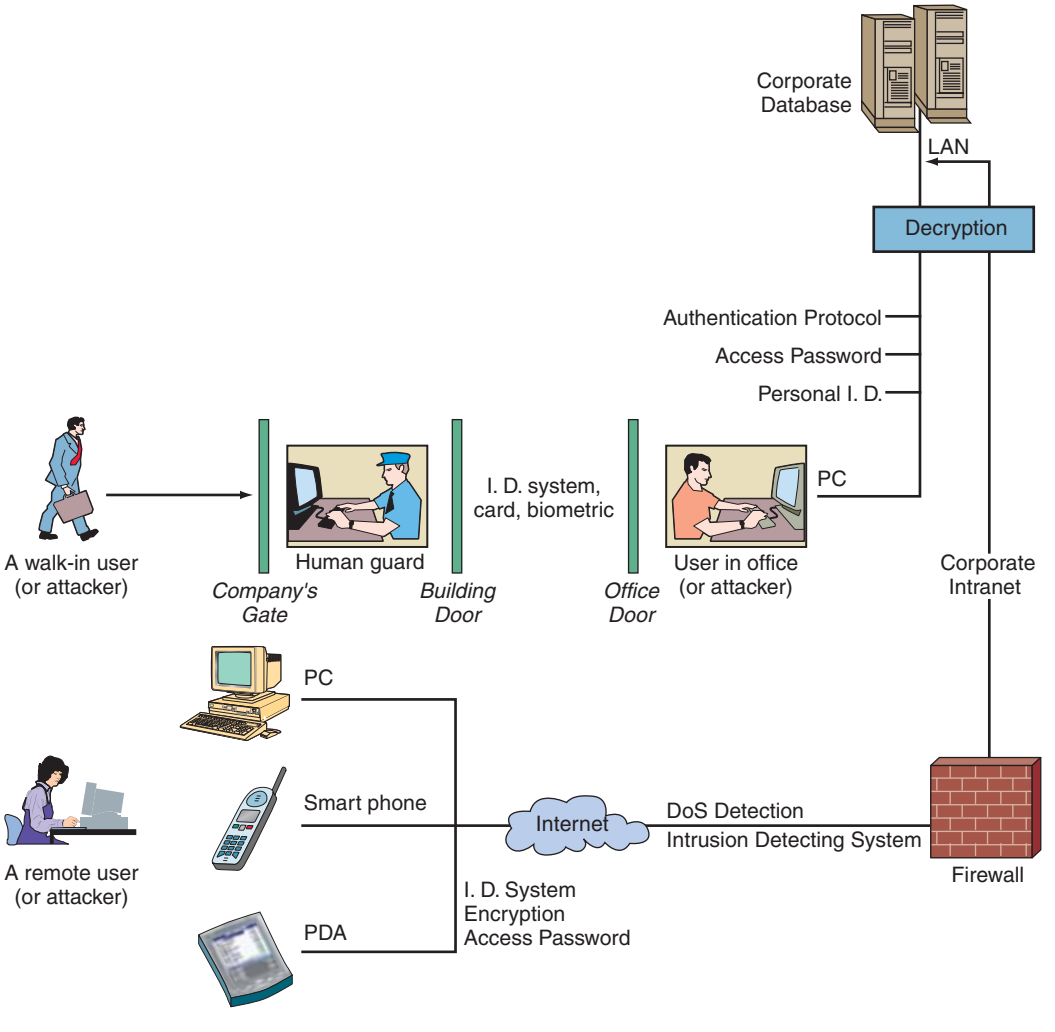


Figure 5.13 IT security mechanisms locations.

All Internet traffic, which travels as packets, should have to pass through a firewall, but that is rarely the case for instant messages and wireless traffic, which, as a result, "carry" malware into the network and applications on host computers. Firewalls do not control anything that happens after a legitimate user (who may be a disgruntled employee or whose username and password have been compromised) has been authenticated and granted authority to access applications on the network. For these reasons, firewalls are a necessary, but insufficient defense.

NETWORK AUTHENTICATION AND AUTHORIZATION

As applied to the Internet, an authentication system guards against unauthorized access attempts. The major objective of authentication is proof of identity. The attempt here is to identify the legitimate user and determine the action he or she is allowed to perform.

Because phishing and identity theft prey on weak authentication, and usernames and passwords do not offer strong authentication, other methods are needed. There are **two-factor authentication** (also called multifactor authentication) and two-tier authentication. With two-factor authentication, other information is used to verify the user's identity, such as biometrics.

There are three key questions to ask when setting up an authentication system:

1. **Who are you?** Is this person an employee, a partner, or a customer? Different levels of authentication would be set up for different types of people.
2. **Where are you?** For example, an employee who has already used a badge to access the building is less of a risk than an employee or partner logging on remotely. Someone logging on from a known IP address is less of a risk than someone logging on from Nigeria or Kazakhstan.
3. **What do you want?** Is this person accessing sensitive or proprietary information or simply gaining access to benign data?

When dealing with consumer-facing applications, such as online banking and e-commerce, strong authentication must be balanced with convenience. If authentication makes it too difficult to bank or shop online, users will go back to the brick and mortars. There is a trade-off between increased protection and turning customers away from your online channel. In addition, authentication of a web site to the customer is equally critical. e-commerce customers need to be able to identify if it is a fraudulent site set up by phishers.

Authorization refers to permission issued to individuals or groups to do certain activities with a computer, usually based on verified identity. The security system, once it authenticates the user, must make sure that the user operates within his or her authorized activities.

SECURING WIRELESS NETWORKS

Wireless networks are more difficult to protect than wired ones. All of the vulnerabilities that exist in a conventional wired network apply to wireless technologies. Wireless access points (wireless APs or WAPs) behind a firewall and other security protections can be a backdoor into a network. Sensitive data that are in clear text (not encrypted) or that are encrypted with a weak cryptographic technique are easily breached.

Major data breaches are initiated by attackers who gained wireless access to organizations from their parking lots or by bypassing organizations' security perimeters by connecting wirelessly to APs inside the organization. Wireless devices used by managers while traveling are infected through remote exploitation during air travel or in cyber cafes. These exploited systems are then used as backdoors when they are reconnected to the network of a target organization. Because they do not require direct physical connections, wireless devices are a convenient vector for attackers to maintain long-term access into a target organization's IT infrastructure.

The SANS Institute (2012) recommends the following controls for wireless networks. For a complete up-to-date listing of critical controls, visit *sans.org/critical-security-controls*.

- Organizations should ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile.
- Organizations should ensure that all wireless APs are manageable using enterprise management tools. APs designed for home use often lack such enterprise management capabilities, and should therefore be avoided in enterprise environments.
- Network vulnerability scanning tools should be configured to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized or rogue APs should be deactivated.
- Organizations should use Wireless Intrusion Detection Systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by a wired IDS as traffic passes into the wired network.
- Organizations should regularly scan for unauthorized or misconfigured wireless infrastructure devices, using techniques such as "war driving" to identify APs and clients accepting peer-to-peer connections. Such unauthorized or misconfigured devices should be removed from the network, or have their configurations altered so that they comply with the security requirements of the organization.

Questions

1. What are network access control (NAC) products?
2. Define perimeter security.
3. Define authorization.
4. What can firewalls not protect against?
5. How can wireless APs put a company at risk?
6. What should organizations do to reduce risks from wireless networks?

5.6 Internal Control and Compliance

The **internal control environment** is the work atmosphere that a company sets for its employees. Internal control is a process designed to achieve:

- Reliability of financial reporting
- Operational efficiency
- Compliance with laws
- Regulations and policies
- Safeguarding of assets

INTERNAL CONTROLS NEEDED FOR COMPLIANCE

The Sarbanes–Oxley Act (SOX) is an antifraud law. It forces more accurate business reporting and disclosure of GAAP (generally accepted accounting principles) violations, thus making it necessary to find and root out fraud. A system of strong internal controls is essential to preventing fraud.

Section 302 deters corporate and executive fraud by requiring that the CEO and CFO verify that they have reviewed the financial report, and, to the best of their knowledge, the report does not contain an untrue statement or omit any material fact. To motivate honesty, executive management faces criminal penalties including long jail terms for false reports. Table 5.5 lists the symptoms, or red flags, of fraud that internal controls can be designed to detect.

Section 805 mandates a review of the Sentencing Guidelines to ensure that "the guidelines that apply to organizations . . . are sufficient to deter and punish organizational criminal conduct." The Guidelines also focus on the establishment of "effective compliance and ethics" programs. As indicated in the Guidelines, a precondition

TABLE 5.5 Indicators of Fraud That Can Be Detected by Internal Controls

- Missing documents
- Delayed bank deposits
- Holes in accounting records
- Numerous outstanding checks or bills
- Disparity between accounts payable and receivable
- Employees who do not take vacations or go out of their way to work overtime
- A large drop in profits
- A major increase in business with one particular customer
- Customers complaining about double billing
- Repeated duplicate payments
- Employees with the same address or telephone number as a vendor

to an effective compliance and ethics program is promotion of "an organizational culture that encourages ethical conduct and a commitment to compliance with the law."

Among other measures, SOX requires companies to set up comprehensive internal controls. There is no question that SOX, and the complex and costly provisions it requires public companies to follow, has had a major impact on corporate financial accounting. For starters, companies have had to set up comprehensive internal controls over financial reporting to prevent fraud and catch it when it occurs. Since the collapse of Arthur Andersen, following the accounting firm's conviction on criminal charges related to the Enron case, outside accounting firms have gotten tougher with clients they are auditing, particularly regarding their internal controls.

SOX and the SEC are making it clear that if controls can be ignored, there is no control. Therefore, fraud prevention and detection require an effective monitoring system.

Approximately 85 percent of insider fraud could have been prevented if proper IT-based internal controls had been designed, implemented, and followed.

SOX requires an enterprise-wide approach to compliance, internal control, and risk management because these issues cannot be dealt with from a departmental or business-unit perspective. However, fraud also requires a worldwide approach, as many incidents have indicated, such as the crime server in Malaysia.

WORLDWIDE ANTI-FRAUD REGULATION

Well-executed insider fraud or money-laundering operations can damage the financial sector, capital markets, and, as a result, a nation's economy. A capital market is any market where a government or a company can raise money to finance operations and long-term investment. Examples are the stock and bond markets.

Preventing internal fraud is high on the political agenda, with the Financial Services Authority (FSA) in the United Kingdom and the SEC in the U.S. both requiring companies to deal with the issue.

Managing risk has become the single most important issue for the regulators and financial institutions. Over the years, these institutions have suffered high costs for ignoring their exposure to risk. However, growing research and improvements in IT have improved the measurement and management of risk.

Questions

1. What is the purpose of an internal control?
2. How does SOX Section 302 attempt to deter fraud?
3. List three symptoms or red flags of fraud that can be detected by internal controls.

5.7 Business Continuity and Auditing

Fires, earthquakes, floods, power outages, and other types of disasters hit data centers. Yet business continuity planning and disaster recovery capabilities can be a tough sell because they do not contribute to the bottom line. Compare them to an insurance policy: if and only if a disaster occurs, the money has been well-spent. And spending on business continuity preparedness can be an open-ended proposition—there is always more that could be done to better prepare the organization.

Ninety-three percent of companies that suffer a significant data loss often go out of business within five years. Disasters may occur without warning, so the best defense is to be prepared. An important element in any security system is the **business continuity plan**, also known as the disaster recovery plan. Such a plan outlines the process by which businesses should recover from a major disaster. Destruction of all (or most) of the computing facilities can cause significant damage. It is difficult for many organizations to obtain insurance for their computers and information systems without showing a satisfactory disaster prevention and recovery plan. IT managers need to estimate how much spending is appropriate for the level of risk an organization is willing to accept.

BUSINESS CONTINUITY PLANNING

Disaster recovery is the chain of events linking the business continuity plan to protection and to recovery. The following are some key thoughts about the process:

- The purpose of a business continuity plan is to keep the business running after a disaster occurs. Each function in the business should have a valid recovery capability plan.
- Recovery planning is part of *asset protection*. Every organization should assign responsibility to management to identify and protect assets within their spheres of functional control.
- Planning should focus first on recovery from a total loss of all capabilities.
- Proof of capability usually involves some kind of what-if analysis that shows that the recovery plan is current.
- All critical applications must be identified and their recovery procedures addressed in the plan.
- The plan should be written so that it will be effective in case of disaster, not just in order to satisfy the auditors.
- The plan should be kept in a safe place; copies should be given to all key managers, or it should be available on the intranet. The plan should be audited periodically.

Disaster recovery planning can be very complex, and it may take several months to complete. Using special software, the planning job can be expedited.

Disaster avoidance is an approach oriented toward prevention. The idea is to minimize the chance of avoidable disasters (such as fire or other human-caused threats). For example, many companies use a device called uninterrupted power supply (UPS), which provides power in case of a power outage.

AUDITING INFORMATION SYSTEMS

An **audit** is an important part of any control system. Auditing can be viewed as an additional layer of controls or safeguards. It is considered as a deterrent to criminal actions, especially for insiders. Auditors attempt to answer questions such as these:

- Are there sufficient controls in the system? Which areas are not covered by controls?
- Which controls are not necessary?
- Are the controls implemented properly?
- Are the controls effective? That is, do they check the output of the system?
- Is there a clear separation of duties of employees?
- Are there procedures to ensure compliance with the controls?
- Are there procedures to ensure reporting and corrective actions in case of violations of controls?

Auditing a web site is a good preventive measure to manage the legal risk. Legal risk is important in any IT system, but in web systems it is even more important due to the content of the site, which may offend people or be in violation of copyright laws or other regulations (e.g., privacy protection). Auditing EC is also more complex since, in addition to the web site, one needs to audit order taking, order fulfillment, and all support systems.

COST-BENEFIT ANALYSIS

It is usually not economical to prepare protection against every possible threat. Therefore, an IT security program must provide a process for assessing threats and deciding which ones to prepare for and which ones to ignore or provide reduced protection against.

Risk-Management Analysis. Risk-management analysis can be enhanced by the use of DSS software packages. A simplified computation is shown here:

$$\text{Expected loss} = P_1 \times P_2 \times L$$

where:

P_1 = probability of attack (estimate, based on judgment)
P_2 = probability of attack being successful (estimate, based on judgment)
L = loss occurring if attack is successful

Example:

$$P_1 = .02, P_2 = .10, L = \$1{,}000{,}000$$

Then, expected loss from this particular attack is

$$P_1 \times P_2 \times L = 0.02 \times 0.1 \times \$1{,}000{,}000 = \$2{,}000$$

The amount of loss may depend on the duration of a system being out of operation. Therefore, some add duration to the analysis.

Ethical Issues. Implementing security programs raises many ethical issues. First, some people are against any monitoring of individual activities. Imposing certain controls is seen by some as a violation of freedom of speech or other civil rights. Handling the privacy versus security dilemma is tough. There are other ethical and legal obligations that may require companies to "invade the privacy" of employees and monitor their actions. In particular, IT security measures are needed to protect against loss, liability, and litigation. Losses are not just financial, but also include the loss of information, customers, trading partners, brand image, and ability to conduct business, due to the actions of hackers, malware, or employees.

Liability stems from two legal doctrines: *respondeat superior* and duty of care. *Respondeat superior* holds employers liable for the misconduct of their employees that occurs within the scope of their employment. With wireless technologies and a mobile workforce, the scope of employment has expanded beyond the perimeters of the company.

Under the doctrine of duty of care, senior managers and directors have a fiduciary obligation to use reasonable care to protect the company's business operations. Litigation, or lawsuits, stem from failure to meet the company's legal and regulatory duties.

Questions

1. Why do organizations need a business continuity plan?
2. List three issues a business continuity plan should cover.
3. Identify two factors that influence a company's ability to recover from a disaster.
4. Explain why business continuity/disaster recovery (BC/DR) is not simply an IT security issue.
5. Why should Web sites be audited?
6. How is expected loss calculated?
7. What is the doctrine of due care?

Key Terms

acceptable use policy (AUP) *128*
administrative controls *133*
advanced persistent threat (APT) attack *117*
adware *129*
Anonymous *118*
application controls *132*
AT&T Toggle *114*
audit *139*
authentication *134*
authorization *134*
availability *123*
baiting *116*
biometrics *123*
botnet *129*
bring your own device (BYOD) to work *133*
business continuity plan *139*
business impact analysis (BIA) *128*
COBIT (Control Objectives for Information and Related Technology) *126*
credentials *117*
confidentiality *123*
consumerization of information technology (COIT) *113*
corporate governance *131*
critical infrastructure *116*
cybersecurity controls *114*
denial of service (DoS) attack *118*
do-not-carry rules *120*
enterprise risk management (ERM) *126*
fault-tolerant system *132*
firewall *124*
general controls *132*
hacktivist *117*
insider fraud *130*
integrity *123*
internal control *127*
internal control environment *137*
internal fraud *130*
internal threats *124*
intrusion detection system (IDS) *124*
IT governance *126*
LulzSec *118*
malware *122*
money laundering *125*
patches *125*
Payment Card Industry Data Security Standard (PCI DSS) *126*
perimeter security *134*
persistent threats *116*
phishing *125*
pretexting *116*
service pack *125*
social engineering *116*
spam *129*
spyware *129*
time-to-exploitation *124*
two-factor authentication *136*
work container *115*
zombies *129*

Chapter 5 LINK LIBRARY

You find clickable Link Libraries for each chapter on the Companion website.

Dark Reading *Darkreading.com*

The *Wall Street Journal* interactive graphic of "China Hackers Hit U.S. Chamber, Attacks Breached Computer System of Business-Lobbying Group; E-mails Stolen," 12/21/2011 *http://online.wsj.com/article/SB10001424052970204058404577110541568535300.html#project%3DCHAMBER122111%26articleTabs%3Dinteractive*

"Video of China Hackers Attack U.S. Chamber of Commerce," 12/21/2011 *http://online.wsj.com/video/china-hackers-attack-us-chamber-of-commerce/A4DF072E-BD65-4063-ABFF-ECB6A9C0312C.html*

Case #3, Cars, Appliances Could Be Hack Targets, 9/9/2011 *http://online.wsj.com/video/cars-appliances-could-be-hack-targets/C1D18429-0F15-4A92-A0B7-418D7760A432.html*

Anti-Phishing Working Group web site *antiphishing.org*

AT&T Toggle video *wireless.att.com/businesscenter/popups/video/learn-more-about-toggle.jsp.*

Government Computer News (GCN) *gcn.com/*

CompTIA *comptia.org/*

SANS Top CyberSecurity Risks *sans.org/top-cyber-security-risks/*

Social engineering *symantec.com/connect/articles/social-engineering*

SANS Institute *20 Critical Controls* *http://www.sans.org/critical-security-controls/*

Evaluate and Expand Your Learning

IT and Data Management Decisions

1. Managers need to determine how much their companies need to invest in cybersecurity to meet their legal obligations. Since there is no such thing as perfect security (i.e., there is always more that you can do), some degree of risk will remain.
   a. When are a company's security measures sufficient to comply with its obligations? For example, does installing a firewall and using virus detection software satisfy a company's legal obligations?
   b. Assume your company has implemented a BYOD solution. Does your company have to encrypt all data that is accessible on employees own devices?
2. Assume that the daily probability of a major earthquake in Los Angeles is .07 percent. The chance of your computer center being damaged during such a quake is 5 percent. If the center is damaged, the average estimated damage will be $1.2 million.
   a. Calculate the expected loss (in dollars).
   b. An insurance agent is willing to insure your facility for an annual fee of $15,000. Analyze the offer, and discuss whether to accept it.
3. Should an employer notify employees that their computer usage and online activities are being monitored by the company? Why or why not?
4. Twenty-five thousand messages arrive at an organization each year. Currently there are no firewalls. On the average there are 1.2 successful hackings each year. Each successful hack attack results in loss to the company of about $130,000. A major firewall is proposed at a cost of $66,000 and a maintenance cost of $5,000. The estimated useful life is 3 years. The chance that an intruder will break through the firewall is 0.0002. In such a case, the damage will be $100,000 (30 percent), or $200,000 (50 percent), or no damage. There is an annual maintenance cost of $20,000 for the firewall.
   a. Would you invest in the firewall? Explain.
   b. An improved firewall that is 99.9988 percent effective and that costs $84,000, with a life of 3 years and annual maintenance cost of $16,000, is available. Should this one be purchased instead of the first one?

Questions for Discussion & Review

1. What are the dangers of BYOD to work, and how can they be minimized?
2. Many firms concentrate on the wrong questions and end up throwing a great deal of money and time at minimal security risks while ignoring major vulnerabilities. Why?
3. Discuss the shift in motivation of criminals.
4. How can the risk of insider fraud be decreased?
5. Why should information control and security be a top concern of management?
6. Explain what firewalls protect and what they do not protect.
7. Why is cybercrime expanding rapidly? Discuss some possible solutions.
8. Some insurance companies will not insure a business unless the firm has a computer disaster recovery plan. Explain why.
9. Explain why risk management should involve the following elements: threats, exposure associated with each threat, risk of each threat occurring, cost of controls, and assessment of their effectiveness.
10. Discuss why the Sarbanes–Oxley Act focuses on internal control. How does that focus influence infosec?

Online Activities

1. Review the *Wall Street Journal* interactive graphic of "China Hackers Hit U.S. Chamber, Attacks Breached Computer System of Business-Lobbying Group; E-mails Stolen" dated December 21, 2011. The link is posted in the Chapter 5 Link Library and is shown here: *http://online.wsj.com/article/SB10001424052970204058404577110541568535300.html#project%3DCHAMBER122111%26articleTabs%3Dinteractive*.
   a. Explain the importance and the role of social engineering in this intrusion and cybertheft.
   b. What can be done to prevent this type of intrusion from occurring again?
2. View the video "China Hackers Attack U.S. Chamber of Commerce" dated December 21, 2011. The WSJ details a cyber attack against the U.S. Chamber of Commerce in which e-mails were stolen. *http://online.wsj.com/video/china-hackers-attack-us-chamber-of-commerce/A4DF072E-BD65-4063-ABFF-ECB6A9C0312C.html*.
   a. Briefly describe the key issues about the intrusion mentioned in the video.
   b. Draft a list of 3 cybersecurity warnings based on the video.
   c. How serious was the intrusion, and when did it occur?
   d. What or whom did the hackers focus on? Why?
   e. What information could the hackers have gleaned from the intrusion of the Chamber?
   f. What did the Chamber do to increase cybersecurity after learning of the intrusion and cybertheft?
   g. Explain why cars and appliances can be hack targets.
   h. What other resources are at risk?
   i. Does this incident indicate about how widespread hacking is? Explain your answer.

Collaborative Work

1. Research a botnet attack. Explain how the botnet works and what damage it causes. What preventive methods are offered by security vendors?
2. The SANS Institute publishes the Top CyberSecurity Risks at *sans.org/top-cyber-security-risks/*.
   a. Which risks would be most dangerous to financial institutions?
   b. Which risks would be most dangerous to marketing firms?
   c. Explain any differences.

3. Access the Anti-Phishing Working Group Web site (*antiphishing.org*) and download the most recent Phishing Activity Trends Report.
   a. Describe the recent trends in phishing attacks.
   b. Explain the reasons for these trends.
4. Research vendors of biometrics. Select one vendor, and discuss three of its biometric devices or technologies. Prepare a list of major capabilities. What are the advantages and disadvantages of its biometrics?

CASE 2 BUSINESS CASE

Army Deploys Androids, Securely

The U.S. government's most IT-security sensitive organizations are the Army and National Security Agency (NSA). The Army and NSA decided to no longer reject mobile technologies or BYOD. Instead these Department of Defense (DoD) organizations looked for secure ways in which commercially available smartphones can be used to access IT systems. Performance and usability are also key concerns particularly because encryption caused latency (delays). Rather than build special handsets that are hardwired with secure components, the DoD choose to install its software on commercially available phones. This approach minimizes costs and allows the government to stay up to date with the latest phones on the market.

Army Selects Customized Androids, Securely

The Army does not permit any type of smartphone. The Army installs its own software on Android phones. Androids were selected because Google allows its code to be modified. The Androids are reengineered to store classified documents, but not to transmit data over a cell network. This approach costs less than building special handsets and makes it easier for the Army to use the latest phones on the market.

The Android needs to be customized to prevent apps from seeking more information than needed to function. For example, a weather or clock app with GPS capabilities identifies a user's location. The Army does not want to support apps that transmit locations over the network.

NSA

Due to the highly classified nature of its work, the NSA has some of the strictest requirements in government, including whole buildings that are labeled as Sensitive Compartmentalized Information Facilities, which have additional requirements.

To comply with strict security requirements, most NSA employees had to leave their mobiles in their cars in the parking lot rather than bringing them in to work. In 2012, the agency worked on a plan to introduce secure, commercially available mobile devices and an architecture that enables other agencies to use mobiles with classified data. Troy Lange, NSA's mobility mission manager explains: "This is about bringing efficiencies and capabilities that people are used to in their everyday lives and extending that to our national security mission."

Questions

1. In your opinion, will the outcome of these Army and NSA projects have a big impact throughout government? On the private sector as well?
2. What are the top three concerns of the DoD?
3. Do you agree that the Army and NSA deciding to allow the use of mobile technologies and to figure out how best to limit risks is encouraging news to the private sector? Explain your answer.
4. Research and describe the latest developments in the Army or NSA's mobile strategy. Does the Army still restrict their mobile strategy to Androids?

CASE 3 VIDEO CASE

Cars, Appliances Could Be Hack Targets

View the video "Cars, Appliances Could Be Hack Targets" on the online *Wall Street Journal* (September 9, 2011; 4 minutes, 44 seconds). *http://online.wsj.com/video/cars-appliances-could-be-hack-targets/C1D18429-0F15-4A92-A0B7-418D7760A432.html*. Officials warn that computers and mobiles are not the only devices vulnerable to hack attacks. Information security risks are expanding to anything attached to a digital network. Vulnerable devices now include cars, appliances, and electricity meters—and will continue to grow. According to the Data Breach Investigations Report (Verizon, Business 2012), most corporate data breaches occur through some type of network device, which makes all networked devices and appliances subject to attack.

Questions

1. Explain why cars, appliances, and other devices not commonly associated with hacking can be hack targets.
2. What other resources are at risk? Why?
3. What are the concerns of the Department of Homeland Security (DHS)?
4. Why is encryption needed?
5. Explain how the capability to remotely control machines creates a vulnerability or a problem in cyberwarfare?

Data Analysis & Decision Making

Financial Impact of Breached Protected Health Information

1. Visit the *HealthDataManagement.com* web site to access the: "Report Assesses the Cost of PHI Breaches," *http://www.healthdatamanagement.com/news/breach-notification-hipaa-privacy-security-44142-1.html*. This report examines the financial impact of breaches of protected health information.
2. Download the free report, which is a collaborative effort of the American National Standards Institute, The Santa Fe Group, and the Internet Security Alliance, with input from more than 100 members of 70 organizations.
3. The report offers "PHIve," a five-step method to calculate the potential or actual cost of a breach. "In addition to the legal and ethical obligations to protect PHI, there is another, very real and equally important reason for protecting it," according to the report. "It is called 'goodwill'—the intangible advantages that a company has in its market, including strategic locations, business connections, and, relevant to this matter, an excellent reputation."
4. Using the five-step method, calculate the potential cost of a breach.

Resources on the Book's Website

More resources and study tools are located on the Student Web Site. You will find additional chapter materials and useful web links. In addition, self-quizzes that provide individualized feedback are available for each chapter.

References

ACFE (Association of Certified Fraud Examiners). acfe.com/. 2012.

Aftergood, S. "Former Official Indicted for Mishandling Classified Info," FAS, April 15, 2010. *fas.org/blog/secrecy/2010/04/drake_indict.html*.

Antilla, S. "Red flags Were There All Along: Suspicious Activities Largely Unquestioned." *Gazette* (Montreal), December 16, 2008.

Chabrow, E. "U.S. Government Takes Up Mobile Challenge." Bankinfosecurity.com, February 7, 2012.

Chickowski, E. "Compliance Policy Development Do's and Don'ts." *Dark Reading*, April 23, 2012.

Dunn, J.E. "Mobile malware up as enterprises take BYOD risks." *Techworld,* April 12, 2012.

Gold, L. "Forensic Accounting: Finding the Smoking E-mail: E-discovery Is Now a Critical Part of Forensics—and of Firm Policy." *Accounting Today* 22(8), May 5, 2008.

Gorman, S. "China Hackers Hit U.S. Chamber." *The Wall Street Journal Online*, December 21, 2011.

Higgins, K. J., "Security's New Reality: Assume the Worst." *Dark Reading,* March 15, 2012.

Hoover, J. N. "National Security Agency Plans Smartphone Adoption." *InformationWeek Government*, February 3, 2012.

Milan, M. "U.S. government, military to get secure Android phones." CNN.com, February 3, 2012. *cnn.com/2012/02/03/tech/mobile/government-android-phones*.

Perloth, N. "Hacked Chamber of Commerce Opposed Cybersecurity Law." *bits.blogs.nytimes.com*, December 21, 2011.

PWC, The 2012 Global State of Information Security Survey. pwc.com/giss2012.

SANS Institute. *20 Critical Controls*, 2012. *http://www.sans.org/critical-security-controls/*.

Verizon Business, "Data Breach Investigations Report (DBIR)." 2012. A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit, and United States Secret Service. *verizonbusiness.com/about/events/2012dbir/index.xml.*