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.*