DISCUSSION QUESTIONS

7.1 Explain how each of the following security procedures can increase system reliability:

1. Encryption
2. Employee security awareness training
3. Firewalls
4. IDS
5. VPNs

7.2 What are the advantages and disadvantages of having the person responsible for information security report directly to the chief information officer (CIO), who has overall responsibility for all aspects of the organization's information systems?

7.3 How much knowledge about information security do internal and external auditors need to be effective?

7.4 Is it possible to provide absolute security for an organization's information system? Why or why not?

7.5 What are the limitations, if any, of relying on the results of penetration tests to assess the overall level of security?

7.6 Security awareness training is necessary to teach employees "safe computing" practices. The key to effectiveness, however, is that it changes employee behavior. How can organizations maximize the effectiveness of their security awareness training programs?

7.7 In what ways can the quest for information security be compared to striving for total quality?

7.8 What are the advantages and disadvantages of biometric security devices, such as fingerprint readers, in comparison with other security measures such as passwords and locked doors?

PROBLEMS

7.1 Which preventive, detective, and/or corrective controls would best mitigate the following threats?

a. An employee's laptop was stolen at the airport. The laptop contained personally identifying information about the company's customers that could potentially be used to commit identity theft.

b. A salesperson successfully logged into the payroll system by guessing the payroll supervisor's password.

c. A criminal remotely accessed a sensitive database using the authentication credentials (user ID and strong password) of an IT manager. At the time the attack occurred, the IT manager was logged into the system at his workstation at company headquarters.

d. An employee received an email purporting to be from her boss informing her of an important new attendance policy. When she clicked on a link embedded in the email to view the new policy, she infected her laptop with a keystroke logger.

e. The director of R&D quit abruptly after an argument with the CEO. The company cannot access any of the files about several new projects because the R&D director had encrypted them before leaving.

f. A company wrote custom code for the shopping cart feature on its Web site. The code contained a buffer overflow vulnerability that could be exploited when the customer typed in the ship-to address.

g. A company purchased the leading "off-the-shelf" e-commerce software for linking its electronic storefront to its inventory database. A customer discovered a way to directly access the back-end database by entering appropriate SQL code.

h. Attackers broke into the company's information system through a wireless access point located in one of its retail stores. The wireless access point had been purchased and installed by the store manager without informing central IT or security.

i. An employee picked up a USB drive in the parking lot and plugged it into their laptop to "see what was on it," which resulted in a keystroke logger being installed on that laptop.

j. A competitor intercepted the company's bid for a lucrative contract that was emailed to the local government's Web site. The competitor used the information contained in the email to successfully underbid and win the contract.

k. When an earthquake destroyed the company's main data center, the CIO spent half a day trying to figure out who in the organization needed to be contacted in order to implement the company's cold site agreement.

l. Although logging was enabled, the information security staff did not review the logs early enough to detect and stop an attack that resulted in the theft of information about a new strategic initiative.

m. To facilitate working from home, an employee installed a modem on his office workstation. An attacker successfully penetrated the company's system by dialing into that modem.

n. An attacker gained access to the company's internal network by installing a wireless access point in a wiring closet located next to the elevators on the fourth floor of a high-rise office building that the company shared with seven other companies.

7.2 EXCEL Problem

Objective: learn how to protect spreadsheets.

Required:

a. Read the article "Keeping Secrets: How to protect your computer from snoops and spies," by Theo Callahan in the July 2007 issue of the *Journal of Accountancy* (available at the AICPA's Web site: www.aicpa.org).

b. Create a new workbook that contains two individual worksheets. On the first worksheet, just enter your name, course number, date, and name of your instructor. On the second worksheet, create the refinancing worksheet as depicted in Exhibit 5 of the *Journal of Accountancy* article.

c. Implement the following controls on the spreadsheet that you created in step b:

a. Password to open
b. Password to modify
c. Apply passwords to each individual worksheet
d. Encrypt the data
e. Set the workbook to be Read-only
f. Protect the appropriate cells in the refinancing worksheet so that they cannot be altered.