Chapter 8

Securing Information Systems

True-False Questions

1. The potential for unauthorized access is usually limited to the entry points of a network.

   Answer: False **Difficulty: Easy** **Reference: p. 316**

2. Computers using a DSL line are generally more vulnerable to outside intruders than older dial-up lines.

   Answer: True **Difficulty: Easy** **Reference: p. 317**

3. The WEP specification calls for users to create unique 40-bit encrypted passwords.

   Answer: False **Difficulty: Hard** **Reference: p. 319**

4. Viruses cannot be spread through e-mail.

   Answer: False **Difficulty: Easy** **Reference: p. 319**

5. A worm is a computer virus that replicates and spreads itself, not only from file to file, but also from computer to computer via e-mail and other Internet traffic.

   Answer: True **Difficulty: Easy** **Reference: p. 319**

6. Trojan horse software is designed to record keystrokes and mouse clicks performed at the computer.

   Answer: False **Difficulty: Medium** **Reference: p. 320**

7. One form of spoofing involves forging the return address on an e-mail so that the e-mail message appears to come from someone other than the sender.

   Answer: True **Difficulty: Medium** **Reference: p. 321**

8. Sniffers enable hackers to steal proprietary information from anywhere on a network, including e-mail messages, company files, and confidential reports.

   Answer: True **Difficulty: Medium** **Reference: p. 321**

9. In a DDoS attack, numerous computers are used to inundate and overwhelm a network from numerous launch points.

   Answer: True **Difficulty: Medium** **Reference: p. 322**

10. *Analysis*

Bot attacks can be prevented by using antivirus and antispyware software.

Answer: False **Difficulty: Medium** **Reference: p. 323**

Analysis in terms of examine

11. The most economically damaging kinds of computer crime are e-mail viruses.

Answer: False **Difficulty: Hard** **Reference: p. 325**

12. Computer forensics experts try to recover ambient data, which are not visible to the average computer user.

Answer: True **Difficulty: Medium** **Reference: pp. 329–330**

13. An acceptable use policy defines the acceptable level of access to information assets for different users.

Answer: False **Difficulty: Medium** **Reference: p. 331**

14. Fault-tolerant computers contain redundant hardware, software, and power supply components.

Answer: True **Difficulty: Easy** **Reference: p. 333**

15. A disaster recovery plan details what you are going to do if disaster strikes and threatens to or actually does knock out your IT system.

Answer: True **Difficulty: Easy** **Reference: p. 333**

16. Biometric authentication is the use of physical characteristics such as retinal images to provide identification.

Answer: True **Difficulty: Easy** **Reference: p. 336**

17. NAT conceals the IP addresses of the organization's internal host computers to deter sniffer programs.

Answer: True **Difficulty: Medium** **Reference: p. 338**

18. Antivirus software can detect and eliminate viruses that are trying to enter your system.

Answer: True **Difficulty: Easy** **Reference: p. 338**

19. SSL is a protocol used to secure information transfer over the Internet.

Answer: True **Difficulty: Easy** **Reference: p. 339**

20. Public key encryption uses mathematically related keys.

Answer: True **Difficulty: Medium** **Reference: p. 341**

Multiple-Choice Questions

21. *Analysis*

The fact that phishing is growing at an explosive rate indicates that:

a. Internet security applications are less able to prevent cyber crime.
b. consumer trust of the Internet is too great.
c. the increasing use of the Internet for online finance is a factor in drawing attention from larger numbers of criminals.
d. consumers need to be educated about phishing and phishing techniques.

Answer: c **Difficulty: Medium** **Reference: p. 314**

Analysis in terms of examine

22. *Evaluation*

What is the most far-reaching effect of identity theft?

a. Corporations implementing more rigorous authentication procedures
b. More governmental control of security standards
c. Lowering of revenues and profits due to public mistrust of e-commerce safety
d. ISPs implementing more active counter-crime techniques

Answer: c **Difficulty: Medium** **Reference: pp. 313–314**

Evaluation in terms of value, assess

23. Policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems refers to:

a. security.
b. controls.
c. benchmarks.
d. algorithms.

Answer: a **Difficulty: Easy** **Reference: p. 316**

24. All of the methods, policies, and organizational procedures that ensure the safety of the organization's assets, the accuracy and reliability of its accounting records, and operational adherence to management standards refers to:

a. legacy systems.
b. SSID standards.
c. vulnerabilities.
d. controls.

Answer: d **Difficulty: Easy** **Reference: p. 316**

25. Large amounts of data stored in electronic form are _____________ than the same data in manual form.

a. less vulnerable to damage
b. more secure
c. vulnerable to many more kinds of threats
d. more critical to most businesses

Answer: c **Difficulty: Easy** **Reference: p. 316**

26. *Evaluation*

Automated data are more susceptible to destruction, fraud, error, and misuse because information systems concentrate data in computer files that:

a. are usually embedded in legacy systems that are easy to access.
b. are not secure because the technology to secure them did not exist at the time the files were created.
c. have the potential to be accessed by large numbers of people and by groups outside of the organization.
d. are frequently available on the Internet.

Answer: c **Difficulty: Medium** **Reference: pp. 316–317**

27. Security challenges posed by the communications between layers in a client/server environment are:

a. line taps and denial of service attacks.
b. tapping, sniffing, and message alteration.
c. computer viruses, line taps, and loss of machine.
d. vandalism, theft and fraud, and line taps.

Answer: b **Difficulty: Hard** **Reference: p. 316**

28. Security challenges specifically faced by corporate servers include:

a. copying of data, alteration of data, and loss of machine.
b. theft and fraud.
c. computer viruses, line taps, and hacking.
d. tapping, sniffing, and message alteration.

Answer: b **Difficulty: Hard** **Reference: p. 316**

29. Computers linked to the Internet are more vulnerable if they are linked through:

a. a cable modem.
b. an ISP.
c. a dial-up line.
d. both a and c.

Answer: a **Difficulty: Medium** **Reference: p. 317**

30. *Evaluation*

The vulnerability inherent in wireless networking is due to:

a. use of the SSIDs.
b. the broadcasting nature of wireless transmission media.
c. the lack of robust encryption capabilities.
d. lack of protection against war driving.

Answer: b **Difficulty: Hard** **Reference: pp. 317–318**

31. An independent computer program that copies itself from one computer to another over a network is called a:

a. worm.
b. Trojan horse.
c. bug.
d. pest.

Answer: a **Difficulty: Easy** **Reference: p. 319**

32. *(Analysis)*

In 2004, ICQ users were enticed by a sales message from a supposed anti-virus vendor. On the vendor's site, a small program called Mitglieder was downloaded to the user's machine. The program enabled outsiders to infiltrate the user's machine. What type of malware is this an example of?

a. Virus
b. Worm
c. Trojan horse
d. Spyware

Answer: c **Difficulty: Medium** **Reference: p. 320**

33. Redirecting a Web link to a different address is a form of:

a. snooping.
b. spoofing.
c. sniffing.
d. phishing.

Answer: b **Difficulty: Easy** **Reference: p. 321**

34. A key logger is a type of:

a. worm.
b. Trojan horse.
c. virus.
d. spyware.

Answer: d **Difficulty: Easy** **Reference: p. 321**

35. Using numerous computers to inundate and overwhelm the network from numerous launch points is called:

a. spamming.
b. spoofing.
c. DDoS.
d. cybervandalism.

Answer: c **Difficulty: Easy** **Reference: p. 322**

36. How do hackers create a botnet?

a. Infecting Web shopping bots with malware
b. Using Web search bots to infect other computers
c. Causing other people’s computers to become “zombie” PCs following a master computer
d. Infecting corporate servers with “zombie” Trojan horses that allow undetected access through a back door

Answer: c **Difficulty: Easy** **Reference: p. 322**

37. *Evaluation*

Which of the following offers the greatest protection against bot attacks?

a. Securing the network properly
b. Alerting employees to virus threats
c. Having individuals use adequate anti-virus protection
d. Having corporations use adequate anti-virus protection

Answer: c **Difficulty: Medium** **Reference: p. 322**

38. *Analysis*

The approach taken by Akamai Technologies when it discovered its servers were under attack illustrates that:

a. enforcing security is a complex endeavor that involves multiple approaches.
b. educating clients about their role in security is paramount.
c. multistep authentication procedures can cause more problems than solutions.
d. anti-virus software must be updated continually to remain effective.

Answer: a **Difficulty: Medium** **Reference: pp. 323–324**

39. Which of the following is an example of a computer used as an instrument of crime?

a. Knowingly accessing a protected computer to commit fraud
b. Accessing a computer system without authority
c. Illegally accessing stored electronic communication
d. Breaching the confidentiality of protected computerized data

Answer: c **Difficulty: Hard** **Reference: p. 324**

40. Phishing involves:

a. redirecting users to a fraudulent Web site even when the user has typed in the correct address in the Web browser.
b. pretending to be a legitimate business's representative in order to garner information about a security system.
c. setting up fake Web sites to ask users for confidential information.
d. using e-mails for threats or harassment.

Answer: c **Difficulty: Medium** **Reference: p. 325**

41. Pharming involves:

a. redirecting users to a fraudulent Web site even when the user has typed in the correct address in the Web browser.
b. pretending to be a legitimate business's representative in order to garner information about a security system.
c. setting up fake Web sites to ask users for confidential information.
d. using e-mails for threats or harassment.

Answer: a **Difficulty: Medium** **Reference: p. 325**

42. Evil twins are:

a. Trojan horses that appears to the user to be a legitimate commercial software application.
b. e-mail messages that mimic the e-mail messages of a legitimate business.
c. fraudulent Web sites that mimic a legitimate business's Web site.
d. bogus wireless networks that look legitimate to users.

Answer: d **Difficulty: Medium** **Reference: p. 325**

43. Tricking employees to reveal their passwords by pretending to be a legitimate member of a company is referred to as:

a. sniffing.
b. social engineering.
c. phishing.
d. pharming.

Answer: b **Difficulty: Easy** **Reference: p. 327**

44. How do software vendors correct flaws in their software after it has been distributed?

a. Issue bug fixes.
b. Issue patches.
c. Re-release software.
d. Issue updated versions.

Answer: b **Difficulty: Easy** **Reference: p. 327**

45. *(Evaluation)*

You have been hired as a security consultant for a legal firm. Which of the following constitutes the greatest threat, in terms of security, to the firm?

a. Wireless network
b. Employees
c. Authentication procedures
d. Lack of data encryption

Answer: b **Difficulty: Medium** **Reference: p. 327**

Evaluation in terms of assess, value

46. Policies, procedures, and tools for managing the retention, destruction, and storage of electronic records is called:

a. ERM.
b. ERD.
c. information policy.
d. information management.

Answer: a **Difficulty: Easy** **Reference: p. 328**

47. The Health Insurance Portability and Accountability Act (HIPAA) of 1996:

a. requires financial institutions to ensure the security of customer data.
b. specifies best practices in information systems security and control.
c. imposes responsibility on companies and management to safeguard the accuracy of financial information.
d. outlines medical security and privacy rules.

Answer: d **Difficulty: Easy** **Reference: p. 328**

48. The Sarbanes-Oxley Act:

a. requires financial institutions to ensure the security of customer data.
b. specifies best practices in information systems security and control.
c. imposes responsibility on companies and management to safeguard the accuracy of financial information.
d. outlines medical security and privacy rules.

Answer: c **Difficulty: Medium** **Reference: p. 329**

49. ISO 17799:

a. requires financial institutions to ensure the security of customer data.
b. specifies best practices in information systems security and control.
c. imposes responsibility on companies and management to safeguard the accuracy of financial information.
d. outlines medical security and privacy rules.

Answer: b **Difficulty: Easy** **Reference: p. 330**

50. The most common type of electronic evidence is:

a. word-processing documents.
b. spreadsheets.
c. instant messages.
d. e-mail.

Answer: d **Difficulty: Medium** **Reference: p. 329**

51. Electronic evidence on computer storage media that is not visible to the average user is called:

a. defragmented data.
b. ambient data.
c. forensic data.
d. recovery data.

Answer: b **Difficulty: Easy** **Reference: pp. 329–330**

52. What is the key issue in information systems security and control?

a. Appropriate use of security software
b. Intelligent management policies
c. Effective employee monitoring and authentication
d. Fault-tolerant computer systems

Answer: b **Difficulty: Medium** **Reference: p. 330**

53. Analysis of an information system that rates the likelihood of a security incident occurring and its cost is included in a(n):

a. security policy.
b. AUP.
c. risk assessment.
d. business impact analysis.

Answer: c **Difficulty: Medium** **Reference: p. 330**

54. Statements ranking information risks are included in a(n):

a. security policy.
b. AUP.
c. risk assessment.
d. business impact analysis.

Answer: a **Difficulty: Medium** **Reference: p. 331**

55. An analysis of the firm's most critical systems and the impact a system's outage would have on the business is included in a(n):

a. security policy.
b. AUP.
c. risk assessment.
d. business impact analysis.

Answer: d **Difficulty: Hard** **Reference: p. 334**

56. A CSO is a:

a. chief security officer.
b. computer security organization.
c. chief systems officer.
d. continuity systems officer.

Answer: a **Difficulty: Easy** **Reference: p. 331**

57. Online transaction processing requires:

a. more processing time.
b. a large server network.
c. fault-tolerant computer systems.
d. a dedicated phone line.

Answer: c **Difficulty: Medium** **Reference: pp. 332–333**

58. Downtime refers to periods of time in which:

a. a computer system is malfunctioning.
b. a computer system is not operational.
c. a corporation is not operational.
d. a computer is not able to perform online transactions.

Answer: b **Difficulty: Easy** **Reference: p. 333**

59. High-availability computing:

a. promises continuous availability.
b. promises the elimination of recovery time.
c. uses online transaction and backup systems.
d. helps firms recover quickly from a crash.

Answer: d **Difficulty: Medium** **Reference: p. 333**

60. Using methods to make computer systems recover more quickly after mishaps is called:

a. high availability computing.
b. recovery oriented computing.
c. fault tolerant computing.
d. disaster-recovery planning.

Answer: b **Difficulty: Medium** **Reference: p. 333**

61. Smaller firms can outsource security functions to:

a. MISs.
b. CSOs.
c. MSSPs.
d. CAs.

Answer: c **Difficulty: Medium** **Reference: p. 334**

62. Rigorous password systems:

a. are one of the most effective security tools.
b. may hinder employee productivity.
c. are costly to implement.
d. are easily disregarded by employees.

Answer: b **Difficulty: Medium** **Reference: p. 336**

63. A token is a(n):

a. device the size of a credit card that contains access permission data.
b. type of smart card.
c. gadget that displays passcodes.
d. electronic marker attached to a digital authorization file.

Answer: c **Difficulty: Medium** **Reference: p. 336**

64. Biometric authentication:

a. is inexpensive.
b. is used widely in Europe for security applications.
c. can use a person’s face as a unique, measurable trait.
d. only uses physical traits as a measurement.

Answer: c **Difficulty: Easy** **Reference: p. 336**

65. A firewall allows the organization to:

a. enforce a security policy on traffic between its network and the Internet.
b. check the accuracy of all transactions between its network and the Internet.
c. create an enterprise system on the Internet.
d. check the content of all incoming and outgoing e-mail messages.

Answer: a **Difficulty: Medium** **Reference: p. 337**

66. In this technique, network communications are analyzed to see whether packets are part of an ongoing dialogue between a sender and a receiver.

a. Stateful inspection
b. Intrusion detection system
c. Application proxy filtering
d. Packet filtering

Answer: a **Difficulty: Medium** **Reference: p. 338**

67. _________ use scanning software to look for known problems such as bad passwords, the removal of important files, security attacks in progress, and system administration errors.

a. Stateful inspections
b. Intrusion detection systems
c. Application proxy filtering technologies
d. Packet filtering technologies

Answer: b **Difficulty: Easy** **Reference: p. 338**

68. Currently, the protocols used for secure information transfer over the Internet are:

a. TCP/IP and SSL.
b. S-HTTP and CA.
c. HTTP and TCP/IP.
d. SSL, TLS, and S-HTTP.

Answer: d **Difficulty: Easy** **Reference: p. 339**

69. In this method of encryption, a single encryption key is sent to the receiver so both sender and receiver share the same key.

a. SSL
b. Symmetric key encryption
c. Public key encryption
d. Private key encryption

Answer: b **Difficulty: Medium** **Reference: p. 339**

70. A digital certificate system:

a. uses third-party CAs to validate a user's identity.
b. uses digital signatures to validate a user's identity.
c. uses tokens to validate a user's identity.
d. are used primarily by individuals for personal correspondence.

Answer: a **Difficulty: Easy** **Reference: p. 342**

Fill in the Blanks

71. Malicious software programs, including threats such as computer viruses, worms, and Trojan horses, are referred to as ***malware*.**

Difficulty: Easy **Reference: p. 319**

72. Small programs that install themselves on computers to monitor user Web surfing activity and serve up advertising are called ***spyware.***

Difficulty: Easy **Reference: p. 321**

73. A(n) ***hacker*** is a person who intends to gain unauthorized entry to a computer system.

Difficulty: Easy **Reference: p. 321**

74. The intentional disruption, defacement, or even destruction of a Web site or corporate information systems is referred to as ***cybervandalism.***

Difficulty: Easy **Reference: p. 321**

75. ***Identify theft*** is a crime in which an imposter obtains key pieces of personal information to impersonate someone else.

Difficulty: Easy **Reference: p. 325**

76. ***Click fraud*** occurs when an individual or computer program fraudulently clicks on an online ad without any intention of learning more about the advertiser or making a purchase.

Difficulty: Easy Reference: p. 326

77. ***Computer forensics*** is the scientific collection, examination, authentication, preservation, and analysis of data held on or retrieved from computer storage media in such a way that the information can be used as evidence in a court of law.

Difficulty: Easy Reference: p. 329

78. A(n) ***MIS audit*** identifies all the controls that govern individual information systems and assesses their effectiveness.

Difficulty: Easy Reference: p. 334

79. ***Access control*** consists of all the policies and procedures a company uses to prevent improper access to systems by unauthorized insiders and outsiders.

Difficulty: Easy Reference: p. 335

80. A(n) ***token*** is a physical device similar to an identification card that is designed to prove the identity of a single user.

Difficulty: Easy Reference: p. 336

Essay Questions

81. *Evaluation*

Hackers and their companion viruses are an increasing problem, especially on the Internet. What can a digital company do to protect itself from this? Is full protection feasible? Why or why not?

For protection, a company must institute good security measures, which include firewalls, investigation of personnel to be hired, physical and software security and controls, antivirus software, and internal education measures. These measures are best put in place at the time the system is designed, and careful attention must be paid to them. A prudent company will engage in disaster protection measures, frequent updating of security software, and frequent auditing of all security measures and of all data upon which the company depends. Full protection may not be feasible in light of the time and expenses involved, but a risk analysis can provide insights into which areas are most important and vulnerable. These are the areas to protect first.

Difficulty: Medium Reference: pp. 330–339

82. . *Evaluation*

Three major concerns of system builders and users are disaster, security, and human error. Of the three, which do you think is most difficult to deal with? Why?

- Disaster might be the most difficult because it is unexpected, broad-based, and frequently life threatening. In addition, the company cannot know if the disaster plan will work until a disaster occurs, and then it's too late to make corrections.
- Security might be the most difficult because it is an ongoing problem, new viruses are devised constantly, and hackers get smarter every day. Furthermore, damage done by a trusted employee from inside cannot be obviated by system security measures.
- Human error might be most difficult because it isn't caught until too late, and the consequences may be disastrous. Also, administrative error can occur at any level and through any operation or procedure in the company.

Difficulty: Medium **Reference: pp. 316–339**

Evaluation in terms of value, judge

83. *Analysis*

Define a fault-tolerant computer system and a high-availability computer system. How do they differ? When would each be used?

Both systems use backup hardware resources. Fault-tolerant computer systems contain extra memory chips, processors, and disk storage devices that can back the system up and keep it running to prevent a system failure. High-availability computing places the emphasis on quick recovery from a system crash. A high-availability system includes redundant servers, mirroring, load balancing, clustering, storage area networks, and a good disaster recovery plan. The main difference between them is that fault-tolerant computer systems don't go down; high-availability computer systems go down, but can recover quickly.

Companies need a technology platform with 100 percent, 24-hr system availability, use fault-tolerant computer systems. High-availability computing environments are a minimum requirement for firms with heavy electronic commerce processing or that depend on digital networks for their internal operations.

Difficulty: Medium **Reference: p. 333**

Analysis in terms of differentiate

84. **Discuss the issue of security challenges on the Internet. List at least 10 Internet security challenges.**

Large public networks, including the Internet, are more vulnerable because they are virtually open to anyone and because they are so huge that when abuses do occur, they can have an enormously widespread impact. When the Internet becomes part of the corporate network, the organization’s information systems can be vulnerable to actions from outsiders. Computers that are constantly connected to the Internet via cable modem or DSL line are more open to penetration by outsiders because they use a fixed Internet address where they can be more easily identified. The fixed Internet address creates the target for hackers. To benefit from electronic commerce, supply chain management, and other digital business processes, companies need to be open to outsiders such as customers, suppliers, and trading partners. Corporate systems must be extended outside the organization so that employees working with wireless and other mobile computing devices can access them. This requires a new security culture and infrastructure, allowing corporations to extend their security policies to include procedures for suppliers and other business partners.

Some of the challenges to Internet security are computer viruses, line taps, loss of the machine itself, tapping, sniffing, message alteration, theft and fraud, hacking, computer viruses, vandalism, denial of service attacks, copying of data, and alteration of data.

Difficulty: Medium **Reference: pp. 316–327**

85. **What is a digital certificate? How does it work?**

A digital certificate is a data file used to establish the identity of people and electronic assets for protection of online transactions. It uses a trusted third party known as a certificate authority or CA to validate a user’s identity. The certificate authority verifies a digital certificate user’s identity offline. This information is put into a CA server, which generates an encrypted digital certificate containing owner identification information and a copy of the owner’s public key. The certificate authority makes its own public key available publicly either in print or on the Internet. The recipient of an encrypted message uses the certificate authority’s public key to decode the digital certificate attached to the message, verifies it was issued by the certificate authority, and then obtains the sender’s public key and identification information contained in the certificate. Using this information, the recipient can send an encrypted reply.

Difficulty: Medium **Reference: p. 342**

86. *Evaluation*

How would the security needs of a large, multinational corporation differ from the needs of a small firm operating from a single office? What security needs would be similar? Which firm would be in a better position to secure its systems, and why?

Student answers will vary but should incorporate the idea that the greater networking needs would introduce more points of vulnerability. An example answer is: A large multinational corporation would probably need to use more networking and the Internet. Both networking technologies and Internet technologies place data in vulnerable places and a large corporation would need to spend more attention on where those vulnerabilities are. However, many of the security needs would be the same, if the small firm was connected to the Internet. The small firm might have an easier time keeping informal track of its employees and their activities, however, the small firm may have less capital to devote to security needs, policies, and technologies for protection.

Difficulty: Medium **Reference: pp. 316–342**

87. **How are encryption, authentication, digital signatures, and digital certificates each used to ensure security?**

- Encryption scrambles a message according to a key, sends the scrambled message, and unscrambles the message at the other end using a matching key.
- Authentication may be achieved through different types of techniques: passwords, biometric data, and digital signatures to confirm the identity of a person.
- Digital signatures are digital codes attached to an electronically transmitted message that are used to verify the origins and content of the message.
- Digital certificates are data files used to establish the identity of people and electronic assets for protection of online transactions. They use a trusted third party to validate the user's identities, with combinations of public and private encryption codes to scramble and unscramble the messages.

Difficulty: Medium **Reference: pp. 335–336, 339–342**

88. *Synthesis*

How can a firm's security policies contribute and relate to the six main business objectives? Give examples.

- **Operational excellence.** Security policies are essential to operational excellence. A firm's daily transactions can be severely disrupted by cybercrime and hackers. A firm's efficiency relies on accurate data.
- **New products, services, business models.** Security policies protect a company's ideas for new products and services, which could be stolen by competitors. Additionally, enhanced security could be seen by a customer as a way to differentiate your product.
- **Customer and supplier intimacy.** Customers rely on your security if they enter personal data into your information system; for example, credit card information into your e-commerce site. The information you receive from customers and suppliers directly affects how able you are to customize your product, service, or communication with them.
- **Improved decision making.** Secure systems make data accuracy a priority, and good decision making relies on accurate and timely data. Lost and inaccurate data would lead to compromised decision making.
- **Competitive advantage.** The knowledge that your firm has superior security than another would, on an otherwise level playing field, make your firm more attractive to do business with. Also, improved decision making, new products and services, which are also affected by security (see above), will contribute to a firm's competitive advantage.
- **Survival.** New laws and regulations make keeping your security system up-to-date a matter of survival. Firms have been destroyed by errors in security policies.

Difficulty: Hard **Reference: pp. 316–342**

Synthesis in terms of model, assemble

89. *Evaluation*

How is the security of a firm's information systems and data affected by its people, organization, and technology? Is the contribution of one of these dimensions any more important than the others? Why?

There are various technological essentials to protecting an information system: firewalls, authentication, encryption, anti-virus protection, etc. Without technology implemented correctly, there is no security. A firm's employees may be its greatest threat, in terms of embezzlement and insider fraud, errors, and lax enforcement of security policies. Probably the most important dimension is organization, because this is what determines a firm's business processes and policies. The firm's information policies can most enhance security by stressing intelligent design of security systems, appropriate use of security technology, the usability of its security processes.

Difficulty: Medium **Reference: pp. 316–342**

Evaluation in terms of assess, compare

90. *Synthesis*

You have just been hired as a security consultant by MegaMalls Inc., a national chain of retail malls, to make sure that the security of their information systems is up to par. Outline the steps you will take to achieve this.

Student answers will vary, but should include an understanding of security assessments, audits, and policies. An example answer is:

1. Establish what data and processes are important and essential to the company.
2. Determine what external and internal information is essential to the different employee roles in the company.
3. Conduct an MIS audit, a security audit, and create a risk assessment analysis.
4. Establish what legal/governmental/industry standards need to be adhered to and which international standards are relevant.
5. Conduct a business impact analysis and determine a disaster recovery and business continuity plan.
6. Create a security policy that defines an acceptable use policy, authorization policies and processes.
7. Plan for any change management needed.
8. Determine how the success of your policy will be measured and set up means for measuring this.
9. Implement such policies
10. Measure and evaluate the effectiveness of the policy and make any additional adjustments.

Difficulty: Hard **Reference: pp. 328–335**

Synthesis in terms of organize, plan