Experiencing MIS, 9e (Kroenke)
Chapter 10 Information Systems Security

1) A(n) ________ is a measure that individuals or organizations take to block a threat from obtaining an asset.
A) denial of service
B) safeguard
C) information silo
D) third-party cookie
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

2) ________ occurs when a threat obtains data that is supposed to be protected.
A) Unauthorized data disclosure
B) Incorrect data modification
C) Faulty service
D) Denial of service
Answer: A
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

3) A person calls the Stark residence and pretends to represent a credit card company. He asks Mrs. Stark to confirm her credit card number. This is an example of ________.
A) hacking
B) data mining
C) pretexting
D) sniffing
Answer: C
AACSB: Reflective Thinking
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Application

4) A ________ pretends to be a legitimate company and sends emails requesting confidential data.
A) hacker
B) phisher
C) wardriver
D) sniffer
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

5) Mark receives an email from his bank asking him to update and verify his credit card details. He replies to the email with all the requested details. Mark later learns that the email was not actually sent by his bank and that the information he had shared has been misused. Mark is a victim of ________.
A) hacking
B) sniffing
C) data mining
D) phishing
Answer: D
AACSB: Reflective Thinking
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Application

6) Which of the following is a synonym for phishing?
A) pretexting
B) email spoofing
C) hardening
D) system hacking
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

7) ________ is a technique for intercepting computer communications.
A) Spoofing
B) Phishing
C) Pretexting
D) Sniffing
Answer: D
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

8) ________ take computers with wireless connections through an area and search for unprotected wireless networks.
A) Wardrivers
B) Pretexters
C) Hackers
D) Phishers
Answer: A
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

9) Breaking into computers, servers, or networks to steal proprietary and confidential data is referred to as ________.
A) pretexting
B) spoofing
C) hacking
D) phishing
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

10) Which of the following occurs when millions of bogus service requests flood a Web server and prevent it from servicing legitimate requests?
A) spoofing
B) incorrect data modification
C) usurpation
D) denial of service
Answer: D
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

11) ________ occurs when computer criminals invade a computer system and replace legitimate programs with their own unauthorized ones.
A) Usurpation
B) Cyber stalking
C) Spoofing
D) Sniffing
Answer: A
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

12) A(n) ________ is a sophisticated, possibly long-running computer hack that is perpetrated by large, well-funded organizations like governments.
A) advanced persistent threat
B) identity threat
C) copyright theft
D) network sniffer attack
Answer: A
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

13) A threat is a person or an organization that seeks to obtain or alter data illegally, without the owner's permission or knowledge.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

14) Pretexting occurs when someone deceives by pretending to be someone else.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

15) Spoofing is a technique for intercepting computer communications.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

16) IP spoofing occurs when an intruder uses another site's IP address to masquerade as that other site.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

17) Wardrivers are those who engage in phishing to obtain unauthorized access to data.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

18) Incorrectly increasing a customer's discount is an example of incorrect data modification.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

19) Advanced persistent threats can be a means to engage in cyber warfare and cyber espionage.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

20) Explain the types of events that result in faulty service, a type of security loss.
Answer: Faulty service includes problems that result because of incorrect system operation. It could include incorrect data modification. It also could include systems that work incorrectly by sending wrong goods to a customer or the ordered goods to a wrong customer, inaccurately billing customers, or sending the wrong information to employees. Humans can inadvertently cause faulty service by making procedural mistakes. System developers can write programs incorrectly or make errors during installation of hardware, software programs, and data. Usurpation is also a type of faulty service. Faulty service can also result when a service is improperly restored during recovery from natural disasters.
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

21) Explain the concept of denial of service (DOS) in information management.
Answer: Human errors in a procedure or a lack of procedures in information management can result in denial of service (DOS). For example, humans can inadvertently shut down a Web server or corporate gateway router by starting a computationally intensive application. Denial-of-service attacks can be launched maliciously. A malicious hacker can flood a Web server, for example, with millions of bogus service requests that so occupy the server that it cannot service legitimate requests. Computer worms can infiltrate a network with so much artificial traffic that legitimate traffic cannot get through. Natural disasters may also cause systems to fail, resulting in denial of service.
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

22) Which of the following statements is TRUE of the financial losses due to computer crimes?
A) All studies on the costs of computer crimes are based on surveys.
B) There are several set standards for tallying computer crime costs and financial losses.
C) Companies are legally required to calculate their financial losses due to computer crime every month.
D) Knowledge about the cost of computer crimes is restricted to large companies.
Answer: A
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.2: How Big Is the Computer Security Problem?
Classification: Concept

23) Damages to security systems caused by natural disasters are minimal when compared to the damages due to human errors.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.2: How Big Is the Computer Security Problem?
Classification: Concept

24) There are no standards for tallying costs of computer crime.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.2: How Big Is the Computer Security Problem?
Classification: Concept

25) A(n) ________ is a computer program that senses when another computer is attempting to scan a disk or access a computer.
A) intrusion detection system
B) adware
C) packet-filtering firewall
D) network security system
Answer: A
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.3: How Should You Respond to Security Threats?
Classification: Concept

26) Which of the following is considered a personal security safeguard?
A) creating backup of cookies and temporary files
B) removing high-value assets from computers
C) using a single valid password for all accounts
D) conducting transactions using http rather than https
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.3: How Should You Respond to Security Threats?
Classification: Concept

27) Davian, a professional hacker, tries every possible combination of characters to crack his victim's email password. Using this technique, he can crack a six-character password of either upper- or lowercase letters in about ten minutes. Which of the following techniques is used by Davian to obtain access to his victim's email?
A) denial-of-service attack
B) brute force attack
C) pretexting
D) spoofing
Answer: B
AACSB: Reflective Thinking
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.3: How Should You Respond to Security Threats?
Classification: Application

28) ________ are small files that browsers store on users' computers when they visit Web sites.
A) Cookies
B) Honeypots
C) Mashups
D) Entity tags
Answer: A
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.3: How Should You Respond to Security Threats?
Classification: Concept

29) In a brute force attack, a password cracker tries every possible combination of characters.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.3: How Should You Respond to Security Threats?
Classification: Concept

30) As one of the safeguards against security threats, a person should preferably use the same password for different sites so as to avoid confusion.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.3: How Should You Respond to Security Threats?
Classification: Concept

31) While making online purchases, a person should buy only from vendors who support https.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.3: How Should You Respond to Security Threats?
Classification: Concept

32) What are some of the recommended personal security safeguards against security threats?
Answer: Some of the recommended personal security safeguards against security threats include the following:
1. Strong passwords should be created.
2. Multiple passwords should be used.
3. Valuable data must not be sent via email or IM.
4. The https at trusted, reputable vendors should be used.
5. High-value assets from computers must be removed.
6. The browsing history, temporary files, and cookies must be cleared.
7. The antivirus software should be updated.
8. Security concern to fellow workers should be demonstrated.
9. The organizational security directives and guidelines must be followed.
10. The security for all business initiatives should be considered.
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.3: How Should You Respond to Security Threats?
Classification: Concept

33) Which of the following is a human safeguard against security threats?
A) encryption
B) firewall
C) physical security
D) procedure design
Answer: D
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.4: How Should Organizations Respond to Security Threats?
Classification: Concept

34) Which of the following is a technical safeguard against security threats?
A) password
B) accountability
C) compliance
D) firewall
Answer: D
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.4: How Should Organizations Respond to Security Threats?
Classification: Concept

35) Which of the following is a data safeguard against security threats?
A) application design
B) accountability
C) physical security
D) malware protection
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.4: How Should Organizations Respond to Security Threats?
Classification: Concept

36) Backup and recovery against computer security threats are ________.
A) technical safeguards
B) data safeguards
C) human safeguards
D) hardware safeguards
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.4: How Should Organizations Respond to Security Threats?
Classification: Concept

37) Risk management is a critical security function addressed by an organization's senior management.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.4: How Should Organizations Respond to Security Threats?
Classification: Concept

38) Financial institutions must invest heavily in security safeguards because they are obvious targets for theft.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.4: How Should Organizations Respond to Security Threats?
Classification: Concept

39) Malware protection is an example of a technical safeguard.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.4: How Should Organizations Respond to Security Threats?
Classification: Concept

40) Hiring, training, and educating employees in an organization is a technical safeguard.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.4: How Should Organizations Respond to Security Threats?
Classification: Concept

41) Technical safeguards include encryption and usage of passwords.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.4: How Should Organizations Respond to Security Threats?
Classification: Concept

42) What are the two critical security functions that an organization's senior management needs to address?
Answer: Senior management in an organization needs to address two critical security functions: security policy and risk management. Considering the first, senior management must establish company-wide security policies. Take, for example, a data security policy that states the organization's posture regarding data it gathers about its customers, suppliers, partners, and employees. At a minimum, the policy should stipulate: what sensitive data the organization will store, how it will process that data, whether data will be shared with other organizations, how employees and others can obtain copies of data stored about them, and how employees and others can request changes to inaccurate data. The specifics of a policy depend on whether the organization is governmental or nongovernmental, on whether it is publicly held or private, on the organization's industry, on the relationship of management to employees, and other factors. The second senior management security function is to manage risk. Risk cannot be eliminated, so to manage risk means to proactively balance the trade-off between risk and cost. This trade-off varies from industry to industry and from organization to organization.
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.4: How Should Organizations Respond to Security Threats?
Classification: Concept

43) To safeguard data against security threats, every information system today requires a user name and a password. In this case, which of the following functions is performed by the user name?
A) authentication
B) identification
C) decryption
D) encryption
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

44) Every information system today should require users to sign on with a user name and a password. In this case, which of the following functions is performed by the user's password?
A) authentication
B) identification
C) decryption
D) encryption
Answer: A
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

45) Which of the following information should be provided by users of smart cards for authentication?
A) personal identification number
B) permanent account number
C) fingerprint
D) retinal scan
Answer: A
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

46) A ________ is a plastic card that has a microchip loaded with identifying data.
A) credit card
B) biometric passport
C) smart card
D) flashcard
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

47) Which of the following uses an individual's personal physical characteristics such as fingerprints, facial features, and retinal scans for verification purposes?
A) credit card
B) smart card
C) biometric authentication
D) symmetric encryption
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

48) ________ is the process of transforming clear text into coded, unintelligible text for secure storage or communication.
A) Usurpation
B) Authentication
C) Malware protection
D) Encryption
Answer: D
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

49) Which of the following statements is TRUE of symmetric encryption?
A) It uses the same key for both encoding and decoding.
B) It is more difficult and slower than asymmetric encryption.
C) It does not require a key to encrypt or decrypt data.
D) It uses a special version called public/private key on the Internet for a secure communication.
Answer: A
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

50) Most secure communications over the Internet use a protocol called ________.
A) smtp
B) ftp
C) https
D) nntp
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

51) With https, data are encrypted using a protocol called the ________.
A) Secure Shell (SSH)
B) Secure Sockets Layer (SSL)
C) File Transfer Protocol (FTP)
D) Post Office Protocol (POP)
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

52) Which of the following types of encryption is used by the secure sockets layer protocol?
A) optical encryption
B) physical layer encryption
C) disk encryption
D) public key encryption
Answer: D
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

53) A(n) ________ sits outside an organizational network and is the first device that Internet traffic encounters.
A) internal firewall
B) perimeter firewall
C) adware
D) malware
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

54) A(n) ________ examines the source address, destination address, and other data of a message and determines whether to let that message pass.
A) encrypted firewall
B) internal malware
C) packet-filtering firewall
D) perimeter shareware
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

55) ________ is a broad category of software that includes viruses, worms, Trojan horses, spyware, and adware.
A) Malware
B) Payload
C) Shareware
D) Firewall
Answer: A
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

56) ________ are viruses that masquerade as useful programs like a computer game, an MP3 file, or some other useful innocuous program.
A) Key loggers
B) Trojan horses
C) Worms
D) Payloads
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

57) Adware and spyware are similar to each other in that they both ________.
A) masquerade as useful programs
B) are specifically programmed to spread
C) are installed with a user's permission
D) reside in the background and observe a user's behavior
Answer: D
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

58) Technical safeguards involve both software and hardware components of an information system.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

59) A username authenticates a user, and a password identifies that user.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

60) Smart cards are convenient to use because they do not require a personal identification number for authentication.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

61) A criticism of biometric authentication is that it provides weak authentication.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

62) With asymmetric encryption, two different keys are used for encoding and decoding a message.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

63) In the case of public key encryption, each site has a private key to encode a message and a public key to decode it.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

64) Packet-filtering firewalls cannot prohibit outsiders from starting a session with any user behind the firewall.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

65) A key is a number used with an encryption algorithm to encrypt data.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

66) Packet-filtering firewalls are the most sophisticated type of firewall.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

67) Spyware programs are installed on a user's computer without the user's knowledge.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

68) Viruses, worms, and Trojan horses are types of firewalls.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

69) A virus is a computer program that replicates itself.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

70) Malware definitions are patterns that exist in malware code.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

71) Discuss briefly the pros and cons of biometric authentication.
Answer: Biometric authentication uses personal physical characteristics such as fingerprints, facial features, and retinal scans to authenticate users. It provides a strong authentication, but the required equipment is expensive. Users often resist biometric identification because they feel it is invasive. Biometric authentication is in the early stages of adoption. Due to its strength, it likely will see increased usage in the future. It is also likely that legislators will pass laws governing the use, storage, and protection requirements for biometric data.
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

72) Explain how secure sockets layer works when a user communicates securely with a Web site.
Answer: Most secure communication over the Internet uses a protocol called https. With https, data are encrypted using a protocol called the Secure Sockets Layer (SSL), which is also known as Transport Layer Security (TLS). SSL/TLS uses a combination of public key encryption and symmetric encryption. Symmetric encryption is fast and is preferred. But the two parties, the user and a Web site, do not share a symmetric key. So, they use public key encryption to share the same symmetric key. The following are the steps involved in this secure communication:
1. A user's computer obtains the public key of a Web site to which it will connect.
2. The user's computer generates a key for symmetric encryption.
3. The user's computer encodes that key using the Web site's public key. It sends the encrypted symmetric key to the Web site.
4. The Web site then decodes the symmetric key using its private key.
5. From that point forward, the user's computer and the Web site communicate using symmetric encryption.
At the end of the session, the user's computer and the secure site discard the keys. Using this strategy, the bulk of the secure communication occurs using the faster symmetric encryption.
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

73) Explain the functions performed by packet-filtering firewalls.
Answer: A packet-filtering firewall examines each part of a message and determines whether to let that part pass. To make this decision, it examines the source address, the destination addresses, and other data. Packet-filtering firewalls can prohibit outsiders from starting a session with any user behind the firewall. They can also disallow traffic from particular sites, such as known hacker addresses. They can prohibit traffic from legitimate, but unwanted, addresses, such as competitors' computers, and filter outbound traffic as well. They can keep employees from accessing specific sites, such as competitors' sites, sites with pornographic material, or popular news sites.
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

74) What are the precautions to be taken when opening email attachments to avoid malwares?
Answer: Users should open email attachments only from known sources. Also, even when opening attachments from known sources, users should do so with great care. With a properly configured firewall, email is the only outside-initiated traffic that can reach user computers. Most antimalware programs check email attachments for malware code. However, all users should form the habit of never opening an email attachment from an unknown source. Also, if users receive an unexpected email from a known source or an email from a known source that has a suspicious subject, odd spelling, or poor grammar, they should not open the attachment without first verifying with the known source that the attachment is legitimate.
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

75) Thomas is responsible for creating backup copies of information in a system. He also works along with IT personnel to ensure that the backups are valid and that effective recovery procedures exist. Thomas is involved in establishing ________.
A) human safeguards
B) data safeguards
C) technical safeguards
D) hardware safeguards
Answer: B
AACSB: Reflective Thinking
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.6: How Can Data Safeguards Protect Against Security Threats?
Classification: Application

76) ________ refers to an organization-wide function that is in charge of developing data policies and enforcing data standards.
A) Database administration
B) Data encapsulation
C) Data administration
D) Database encapsulation
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.6: How Can Data Safeguards Protect Against Security Threats?
Classification: Concept

77) The procedure of entrusting a party with a copy of an encryption key that can be used in case the actual key is lost or destroyed is called ________.
A) key escrow
B) pledged encryption
C) insured encryption
D) key replication
Answer: A
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.6: How Can Data Safeguards Protect Against Security Threats?
Classification: Concept

78) The loss of encryption keys by employees is referred to as key escrow.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.6: How Can Data Safeguards Protect Against Security Threats?
Classification: Concept

79) The creation of backup copies of database contents makes the data more vulnerable to security threats.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.6: How Can Data Safeguards Protect Against Security Threats?
Classification: Concept

80) Explain the functions of the two organizational units responsible for data safeguarding.
Answer: Data safeguards protect databases and other organizational data. Two organizational units are responsible for data safeguards–data administration and database administration. Data administration refers to an organization-wide function that is in charge of developing data policies and enforcing data standards. Database administration refers to a function that pertains to a particular database. ERP, CRM, and MRP databases each have a database administration function. Database administration develops procedures and practices to ensure efficient and orderly multiuser processing of the database, to control changes to the database structure, and to protect the database. Both data and database administration are involved in establishing data safeguards. First, data administration should define data policies. Then, data administration and database administrations work together to specify user data rights and responsibilities. Third, those rights are enforced by user accounts that are authenticated at least by passwords.
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.6: How Can Data Safeguards Protect Against Security Threats?
Classification: Concept

81) Which of the following statements is TRUE of position sensitivity?
A) It protects sensitive data by storing it in specific encrypted form.
B) It enables security personnel to prioritize their activities in accordance with the possible risk and loss.
C) It refers to the specific documentation of highly influential and sensitive positions in an administration.
D) It increases the effectiveness of user accounts by giving users the maximum possible privilege needed to perform their job.
Answer: B
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.7: How Can Human Safeguards Protect Against Security Threats?
Classification: Concept

82) Which of the following are the three independent factors that constitute the enforcement of security procedures and policies?
A) centralized reporting, preparation, and practice
B) hiring, screening, and terminating
C) separation of duties, provision of maximum privilege, and position sensitivity
D) responsibility, accountability, and compliance
Answer: D
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.7: How Can Human Safeguards Protect Against Security Threats?
Classification: Concept

83) ________ a site means to take extraordinary measures to reduce a system's vulnerability.
A) Pretexting
B) Hacking
C) Spoofing
D) Hardening
Answer: D
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.7: How Can Human Safeguards Protect Against Security Threats?
Classification: Concept

84) In terms of password management, when an account is created, users should ________.
A) create two passwords and switch back and forth between the two
B) immediately change the password they are given to a password of their own
C) maintain the same password they are given for all future authentication purposes
D) ensure that they do not change their passwords frequently to reduce the risk of password theft
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.7: How Can Human Safeguards Protect Against Security Threats?
Classification: Concept

85) ________ are created by companies as false targets for computer criminals to attack.
A) Negatives
B) Honeypots
C) Cookies
D) Trojan horses
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.7: How Can Human Safeguards Protect Against Security Threats?
Classification: Concept

86) In an organization, security sensitivity for each position should be documented.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.7: How Can Human Safeguards Protect Against Security Threats?
Classification: Concept

87) Existence of accounts that are no longer necessary does not pose a security threat.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.7: How Can Human Safeguards Protect Against Security Threats?
Classification: Concept

88) A help-desk information system has answers to questions that only a true user of an account or system would know.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.7: How Can Human Safeguards Protect Against Security Threats?
Classification: Concept

89) Explain how defining positions in an organization can safeguard against security threats.
Answer: Effective human safeguards begin with definitions of job tasks and responsibilities. In general, job descriptions should provide a separation of duties and authorities. For example, no single individual should be allowed to both approve expenses and write checks. Instead, one person should approve expenses, another pay them, and a third should account for the payment. Similarly, in an inventory, no single person should be allowed to authorize an inventory withdrawal and also to remove the items from the inventory. Given appropriate job descriptions, user accounts should be defined to give users the least possible privilege needed to perform their jobs. Similarly, user accounts should prohibit users from accessing data their job description does not require. Because of the problem of semantic security, access to even seemingly innocuous data may need to be limited. Finally, security sensitivity should be documented for each position. Some jobs involve highly sensitive data. Other positions involve no sensitive data. Documenting position sensitivity enables security personnel to prioritize their activities in accordance with the possible risk and loss.
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.7: How Can Human Safeguards Protect Against Security Threats?
Classification: Concept

90) What human safeguards should be taken against security threats for temporary personnel, vendors, and partner personnel?
Answer: Business requirements may necessitate opening information systems to nonemployee personnel–temporary personnel, vendors, partner personnel (employees of business partners), and the public. In the case of temporary, vendor, and partner personnel, a contract that governs an activity should call for security measures appropriate to the sensitivity of data and information system resources involved. Companies should require vendors and partners to perform appropriate screening and security training. The contract also should mention specific security responsibilities that are particular to the work to be performed. Companies should provide accounts and passwords with the least privilege and remove those accounts as soon as possible. Although temporary personnel can be screened, to reduce costs the screening will be abbreviated from that for employees. But in most cases, companies cannot screen either vendor or partner personnel. Public users cannot be screened at all.
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.7: How Can Human Safeguards Protect Against Security Threats?
Classification: Concept

91) A(n) ________ includes how employees should react to security problems, whom they should contact, the reports they should make, and steps they can take to reduce further loss.
A) application design
B) activity log
C) systems procedure
D) incident-response plan
Answer: D
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.8: How Should Organizations Respond to Security Incidents?
Classification: Concept

92) Incident-response plans should provide centralized reporting of all security incidents.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.8: How Should Organizations Respond to Security Incidents?
Classification: Concept

93) Describe an incident-response plan.
Answer: Every organization should have an incident-response plan as part of its security program. The plan should include how employees are to respond to security problems, whom they should contact, the reports they should make, and steps they can take to reduce further loss. The plan should provide centralized reporting of all security incidents that will enable an organization to determine if it is under systematic attack or whether an incident is isolated. Centralized reporting also allows the organization to learn about security threats, take consistent actions in response, and apply specialized expertise to all security problems. Viruses and worms can spread very quickly across an organization's networks, and a fast response will help to mitigate the consequences. Owing to the need for speed, preparation pays. The incident-response plan should identify critical personnel and their off-hours contact information. These personnel should be trained on where to go and what to do when they get there. Finally, organizations should periodically practice incident response.
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.8: How Should Organizations Respond to Security Incidents?
Classification: Concept

94) Jack installed the incorrect security patch on the server. This is an example of what type of security problem?
A) denial of service
B) faulty service
C) hacking
D) malicious third-party cookie
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

95) Which is NOT an example of a natural disaster?
A) flood
B) power outage
C) earthquakes
D) hurricanes
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

96) When is the most opportune time for a hacker to steal data?
A) when someone is performing data modification
B) during a data backup
C) early in the morning
D) while IT is restoring data due to a natural disaster
Answer: D
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

97) Which of the following is the most expensive consequence of computer crime?
A) information loss
B) business disruption
C) equipment losses and damage
D) recovery
Answer: A
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.2: How Big Is the Computer Security Problem?
Classification: Concept

98) Companies that spend more time on safeguards experience less computer crime.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.2: How Big Is the Computer Security Problem?
Classification: Concept

99) There are standards to assist a company in determining the loss if a computer crime occurs.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.2: How Big Is the Computer Security Problem?
Classification: Concept

100) Currently, which of the following is NOT true about computer crime according to the Ponemon study?
A) Social engineering are increasing serious security threats.
B) Data loss and business disruption are principal costs of computer crime.
C) Detection and recovery account for over half of the internal costs related to cyber intrusions.
D) Security safeguards don't work.
Answer: D
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.2: How Big Is the Computer Security Problem?
Classification: Concept

101) Which of the following type of password guidelines are the easiest to crack?
A) a six-letter password with upper and lower-case letters
B) a ten-digit password with only uppercase letters
C) a password with special characters
D) a twelve-digit password with letters only
Answer: A
AACSB: Reflective Thinking
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.3: How Should You Respond to Security Threats?
Classification: Application

102) What should one look for when engaging in online shopping to shop safely?
A) a http connection
B) a https connection
C) only if the product is sold Amazon
D) All vendors are safe.
Answer: B
AACSB: Reflective Thinking
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.3: How Should You Respond to Security Threats?
Classification: Application

103) What is one of the drawbacks of removing and disabling cookies?
A) Hackers will have increased access to data on the computer.
B) It will slow down the process of loading websites on your computer.
C) Your computer will be harder to use.
D) You will not have to sign in every time you visit a website.
Answer: C
AACSB: Reflective Thinking
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.3: How Should You Respond to Security Threats?
Classification: Application

104) What are the minimum items a company-wide security policy should address?
Answer: At a minimum, the policy should stipulate:

- What sensitive data the organization will store
- How it will process that data
- Whether data will be shared with other organizations
- How employees and others can obtain copies of data stored about them
- How employees and others can request changes to inaccurate data

AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.4: How Should Organizations Respond to Security Threats?
Classification: Concept

105) Which of the following is an example of a data safeguard?
A) firewalls
B) compliance
C) physical security
D) hiring
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.4: How Should Organizations Respond to Security Threats?
Classification: Concept

106) The specifics of a policy depend on whether the organization is governmental or nongovernmental.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.4: How Should Organizations Respond to Security Threats?
Classification: Concept

107) A ________ is a string of bits used to encrypt the data.
A) secure socket layer
B) transport security layer
C) firewall
D) key
Answer: D
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

108) The ________ can delete programs or data or even modify data in undetected ways.
A) virus
B) trojan horse
C) payload
D) spyware
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

109) Describe how a computer may show signs of spyware and/or adware symptoms.
Answer: Answers may vary.

- Slow system startup
- Sluggish system performance
- Many pop-up advertisements
- Suspicious browser homepage changes
- Suspicious changes to the taskbar and other system interfaces
- Unusual hard disk activity

AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

110) What can a company do to safeguard their data?
Answer: • Define data policies

- Data rights and responsibilities
- Rights enforced by user accounts authenticated by passwords
- Data encryption
- Backup and recovery procedures
- Physical security

AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.6: How Can Data Safeguards Protect Against Security Threats?
Classification: Concept

111) Both data and database administration are involved in establishing the data safeguards.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.6: How Can Data Safeguards Protect Against Security Threats?
Classification: Concept

112) What should a company store off premise preferably in a remote location?
A) private keys
B) servers
C) backup copies of data
D) escrow
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.6: How Can Data Safeguards Protect Against Security Threats?
Classification: Concept

113) Which of the following is a task for the system user during the recovery system procedure?
A) Prepare for the loss of system functionality.
B) Recover systems from the backed-up data.
C) Accomplish job tasks during failure.
D) Operate data center equipment.
Answer: C
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.7: How Can Human Safeguards Protect Against Security Threats?
Classification: Concept

114) After Equifax was hacked, they went through ________ process to reduce the system's vulnerability.
A) a cleansing project
B) a new management hiring process
C) a hardening
D) a honeypot process
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.7: How Can Human Safeguards Protect Against Security Threats?
Classification: Concept

115) Which of the following is a primary means of authentication?
A) passwords
B) fingerprints
C) hardening
D) termination
Answer: A
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.7: How Can Human Safeguards Protect Against Security Threats?
Classification: Concept

116) All of the following are factors in incident response EXCEPT ________.
A) have a plan in place
B) practice
C) don't make the problem worse
D) take your time responding to the incident
Answer: D
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.8: How Should Organizations Respond to Security Incidents?
Classification: Concept

117) When an incident does occur, speed is of the essence.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.8: How Should Organizations Respond to Security Incidents?
Classification: Concept

118) The Grey-Sloan hospital was attached by a virus. The interns should check the ________ for next steps.
A) honeypot
B) activity log
C) disaster recovery procedures
D) incident-response plan
Answer: D
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.8: How Should Organizations Respond to Security Incidents?
Classification: Concept

119) Information security is a trade-off between ________.
A) security and freedom
B) cost and security
C) time and money
D) employer and employee
Answer: A
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.1: What Is the Goal of Information Systems Security?
Classification: Concept

120) Why is it difficult to rely on the accuracy of computer crime cost estimates?
A) Organizations report all of their losses.
B) Because ransomware is decreasing.
C) Because there is only one company that reports computer crime.
D) There are no standard definitions for reporting computer crime.
Answer: D
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.2: How Big Is the Computer Security Problem?
Classification: Concept

121) What type of data is okay to send in an instant message?
A) passwords
B) a RSVP to a wedding
C) credit card numbers
D) username
Answer: B
AACSB: Reflective Thinking
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.3: How Should You Respond to Security Threats?
Classification: Application

122) Which business incurs the most risk for not having a strong security policy?
A) a bowling alley
B) a bakery
C) a bank
D) a car
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.4: How Should Organizations Respond to Security Threats?
Classification: Concept

123) As an IS user who is not designing programs, what should a person ensure of any future applications?
A) Make sure there are data disclosures located around the building.
B) Design a firewall into each system
C) Make sure the data is stored in the cloud.
D) Make sure to include security as a requirement.
Answer: D
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.5: How Can Technical Safeguards Protect Against Security Threats?
Classification: Concept

124) If a company stores client credit card data on an unsecured PC in the office, the company is violating which law?
A) Gramm-Leach-Bliley Act (GLBA)
B) Health Insurance Portability and Accountability Act (HIPAA)
C) Payment Card Industry Data Security Standard (PCI DSS)
D) The Privacy Principles of the Australian Privacy Act of 1988
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.6: How Can Data Safeguards Protect Against Security Threats?
Classification: Concept

125) There is no difference concerning human safeguards between temporary and full-time employees.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.7: How Can Human Safeguards Protect Against Security Threats?
Classification: Concept

126) If an organizations honeypot is attacked, the organization can not trace the IP address back to the attacker.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO 10.8: How Should Organizations Respond to Security Incidents?
Classification: Concept