09

Student: _____

1. What is the recommended way to implement information security lines of defence?
   A. People first, technology second
   B. Technology first, people second
   C. None of the above
   D. All of the above

2. Which term describes legitimate users who purposely or accidentally misuse their access to the environment and cause some kind of business-affecting incident?
   A. Hactivist
   B. Social engineering
   C. Insiders
   D. Virus

3. What identifies the rules required to maintain information security?
   A. Information security plan
   B. Information security policies
   C. Authentication
   D. Biometrics

4. Which of the following is not one of the five steps for creating an information security plan?
   A. Develop the information security policies
   B. Communicate the information security policies
   C. Revise and test the information security policies
   D. Test and reevaluate risks

5. What is social engineering?
   A. Using one's social skills to trick people into revealing access credentials or other information valuable to the attacker
   B. Legitimate users who purposely or accidentally misuse their access to the environment and cause some kind of business-affecting incident
   C. Small electronic devices that change user passwords automatically
   D. A method for confirming user's identities

6. Which of the following is not one of the top 10 questions managers should ask regarding information security?
   A. Is there clear accountability for information security in our organization?
   B. How much is spent on information security and what is it being spent on?
   C. What is the impact on the organization of a serious security incident?
   D. How do we identify potential insiders?

7. Which of the following is not one of the three primary information security areas?
   A. Authentication and authorization
   B. Prevention and resistance
   C. Detection and resistance
   D. None of the above

8. What is a method for confirming users' identities?
   A. Authentication
   B. Prevention
   C. Detection
   D. Response

9. What is the most secure type of authentication?
   A. Something the user knows such as a user ID and password
   B. Something the user has such as a smart card or token
   C. Something that is part of the user such as a fingerprint or voice signature
   D. Combination of all of the above

10. What is a device that is around the same size as a credit card, containing embedded technologies that can store information and small amounts of software to perform some limited processing?
   A. Token
   B. Password
   C. Smart card
   D. Biometrics

11. What is the identification of a user based on a physical characteristic, such as a fingerprint, iris, face, voice, or handwriting?
   A. Smart card
   B. Token
   C. Biometrics
   D. Content filtering

12. Which of the following is considered a type of biometrics?
   A. Voice
   B. Face
   C. Iris
   D. All of the above

13. What is the most costly and intrusive form of authentication?
   A. Something the user knows such as a user ID and password
   B. Something the user has such as a smart card or token
   C. Something that is part of the user such as a fingerprint or voice signature
   D. None of the above

14. Which of the following authentication methods is 100 percent accurate?
   A. Smart card
   B. Fingerprint authentication
   C. User ID
   D. None of the above

15. What are the technologies available to help prevent and build resistance to attacks?
   A. Content filtering, encryption, firewalls
   B. Content filtering, encryption, insiders
   C. Encryption, firewalls, insiders
   D. Firewalls, social engineering, encryption

16. What occurs when an organization uses software that filters content to prevent the transmission of unauthorized information?
   A. Biometrics
   B. Encryption
   C. Firewalls
   D. Content Filtering

17. What is spam?
   A. A type of encryption
   B. A type of content filtering
   C. A form of unsolicited e-mail
   D. None of the above

18. What is encryption?
    A. Occurs when an organization uses software that filters content to prevent the transmission of unauthorized information
    B. Scrambles information into an alternative form that requires a key or password to decrypt the information
    C. Hardware and/or software that guards a private network by analyzing the information leaving and entering the network
    D. A form of unsolicited e-mail

19. Which of the following can be completed by encryption?
    A. Switch the order of characters
    B. Replace characters with other characters
    C. Use a mathematical formula to convert the information into some sort of code
    D. All of the above

20. Where do organizations typically place firewalls?
    A. Between a personal computer and the server
    B. Between a personal computer and a printer
    C. Between the server and the content filtering software
    D. Between the server and the Internet

21. Which of the following does a firewall perform?
    A. Examines each message that wants entrance to the network
    B. Blocks messages without the correct markings from entering the network
    C. Detects computers communicating with the Internet without approval
    D. All of the above

22. What includes a variety of threats such as viruses, worms, and Trojan horses?
    A. Malicious code
    B. Hoaxes
    C. Spoofing
    D. Sniffer

23. What is the forging of the return address on an e-mail so that the e-mail message appears to come from someone other than the actual sender?
    A. Malicious code
    B. Hoaxes
    C. Spoofing
    D. Sniffer

24. Which of the following is a program or device that can monitor data traveling over a network?
    A. Malicious code
    B. Hoaxes
    C. Spoofing
    D. Sniffer

25. What attacks computer systems by transmitting a virus hoax, with a real virus attached?
    A. Malicious code
    B. Hoaxes
    C. Spoofing
    D. Sniffer

26. What is the most common type of defence within detection and response technologies?
    A. Malicious code
    B. Token
    C. User ID
    D. Antivirus software

27. Who works at the request of the system owners to find system vulnerabilities and plug the holes?
    A. White-hat hackers
    B. Black-hat hackers
    C. Hactivists
    D. Script kiddies

28. Who breaks into other people's computer systems and just looks around or steals and destroys information?
    A. White-hat hacker
    B. Black-hat hacker
    C. Hactivists
    D. Script kiddies

29. Who finds hacking code on the Internet and click-and-points their way into systems to cause damage or spread viruses?
    A. White-hat hacker
    B. Black-hat hacker
    C. Hactivists
    D. Script kiddies

30. Who are hackers with criminal intent?
    A. White-hat hacker
    B. Black-hat hacker
    C. Crackers
    D. Cyberterrorists

31. Who are those who seek to cause harm to people or to destroy critical systems or information and use the Internet as a weapon of mass destruction?
    A. White-hat hacker
    B. Black-hat hacker
    C. Crackers
    D. Cyberterrorists

32. What is a type of virus that spreads itself, not just from file to file, but also from computer to computer?

    A. Computer virus
    B. Worm
    C. Denial-of-service attack
    D. None of the above

33. What floods a Web site with so many requests for service that it slows down or crashes the site?
    A. Computer virus
    B. Worm
    C. Denial-of-service attack
    D. None of the above

34. Which is a virus that opens a way into the network for future attacks?
    A. Distributed denial-of-service attack
    B. Worm
    C. Denial-of-service attack
    D. Backdoor programs

35. If there is a security breech on your organizational information systems, which information security area is best suited to handle the breech?
    A. Authentication and authorization
    B. Prevention and resistance
    C. Detection and response
    D. Detection and resistance

36. What are the principles and standards that guide our behaviour toward other people?
A. Ethics
B. Intellectual property
C. Copyright
D. Fair Use Doctrine

37. What is intangible creative work that is embodied in physical form?
A. Ethics
B. Intellectual property
C. Copyright
D. Fair Use Doctrine

38. What is the legal protection afforded an expression of an idea, such as a song, video game, and some types of proprietary documents?
A. Ethics
B. Intellectual property
C. Copyright
D. Fair Use Doctrine

39. What is it called when you may use copyrighted material in certain situations—for example, in the creation of new work or, within certain limits, for teaching purposes?
A. Ethics
B. Intellectual property
C. Copyright
D. Fair dealing

40. What is the right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent?
A. Fair Use Doctrine
B. Pirated software
C. Counterfeit software
D. Privacy

41. What is software that is manufactured to look like the real thing and sold as such?
A. Fair Use Doctrine
B. Pirated software
C. Counterfeit software
D. Privacy

42. What is the unauthorized use, duplication, distribution, or sale of copyrighted software?
A. Fair Use Doctrine
B. Pirated software
C. Counterfeit software
D. Privacy

43. What are the policies and procedures that address the ethical use of computers and Internet usage in the business environment?
A. Ethics
B. ePolicies
C. All of the above
D. None of the above

44. Which of the following describes privacy?
A. The assurance that messages and data are available only to those who are authorized to view them
B. Policies and procedures that address the ethical use of computers and Internet usage in the business environment
C. The right to be left alone when you want to be, to have control over your own personal possessions, and to not be observed without your consent
D. The principles and standards that guide our behaviour toward other people

45. Which of the following describes confidentiality?
A. The assurance that messages and information are available only to those who are authorized to view them
B. Policies and procedures that address the ethical use of computers and Internet usage in the business environment
C. The right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent
D. The principles and standards that guide our behaviour toward other people

46. Which of the following describes ePolicies?
A. The assurance that messages and data are available only to those who are authorized to view them.
B. Policies and procedures that address the ethical use of computers and Internet usage in the business environment
C. The right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent
D. The principles and standards that guide our behaviour toward other people

47. Which of the following is not considered an ePolicy?
A. Acceptable use policy
B. Internet use policy
C. Ethical computer use policy
D. None of the above

48. Which of the following is an example of acting ethically?
A. Individuals copy, use, and distribute software
B. Employees search organizational databases for sensitive corporate and personal information.
C. Individuals hack into computer systems to steal proprietary information.
D. None of the above

49. Which of the following is not included in the four quadrants of ethical and legal behaviour?
A. Legal behaviour and ethical behaviour
B. Illegal behaviour and ethical behaviour
C. Legal behaviour and unethical behaviour
D. None of the above

50. What is the ideal type of decisions for people in an organization to make?
A. Legal and ethical
B. Illegal and ethical
C. Legal and unethical
D. Illegal and unethical

51. What was the primary problem Saab encountered with one of its marketing companies?
A. Contacted customers based on opt-out decision
B. Contacted customers based on opt-in decision
C. Contacted customers regardless of their opt-out or opt-in decision
D. Failed to contact any customers

52. What is a small file deposited on a hard drive by a Web site containing information about customers and their Web activities?
A. Key logger
B. Hardware key logger
C. Cookie
D. Adware

53. Which of the following is an effect of employee monitoring?
A. Employee absenteeism is on the rise.
B. Job satisfaction is on the rise.
C. Psychological reactance is prevented.
D. All of the above.

54. Canada's privacy laws follow very closely to the:
    A. European model
    B. US model
    C. Bork model
    D. None of the above

55. Which of the following is not one of the 10 Guiding principals of PIPEDA for organizations:
    A. Accountability
    B. Accuracy
    C. Open access
    D. Safeguards

56. Which of the following is/are covered by Canada's Privacy Act:
    A. medical records
    B. security clearances
    C. tax records
    D. All of the above

57. Which of the following is not one of the six principles for ethical information management according to CIO magazine?
    A. Information is a valuable corporate asset and should be managed as such
    B. The CIO is responsible for controlling access to and use of information
    C. The CIO is responsible for preventing the inappropriate destruction of information
    D. The CIO is responsible for how outsiders view and analyze corporate information

58. What is the policy that contains general principles to guide computer user behaviour?
    A. Information privacy policy
    B. Acceptable use policy
    C. Internet use policy
    D. None of the above

59. Which policy ensures that the users know how to behave at work and that the organization has a published standard through which to deal with user infractions?
    A. Information privacy policy
    B. Acceptable use policy
    C. Internet use policy
    D. Ethical computer use policy

60. According to the ethical computer use policy, users should be _____ of the rules and, by agreeing to use the system on that basis, _____ to abide by the rules.
    A. Informed, collaborate
    B. Consent, informed
    C. Informed, consent
    D. None of the above

61. If an organization were to have only one policy, which one would it want?
    A. Information privacy policy
    B. Acceptable use policy
    C. Internet use policy
    D. Ethical computer use policy

62. Which policy contains general principles regarding information privacy?
    A. Information privacy policy
    B. Acceptable use policy
    C. Internet use policy
    D. Anti-Spam policy

63. Which of the following represents the classic example of unintentional information reuse?
    A. Phone number
    B. Social Security number
    C. Address
    D. Driver's license number

64. What is one of the guidelines an organization can follow when creating an information privacy policy?

    A. Adoption and implementation of an anti-spam policy
    B. Notice and disclosure
    C. Choice and quality
    D. None of the above

65. What is a policy that a user must agree to follow in order to be provided access to a network or to the Internet?
    A. Ethical computer use policy
    B. Acceptable use policy
    C. Nonrepudiation policy
    D. None of the above

66. What is a contractual stipulation that ensures that e-business participants do not deny their online actions?

    A. Copyright
    B. Fair use doctrine
    C. Nonrepudiation
    D. Intellectual property

67. Which policy typically contains a nonrepudiation clause?
    A. Ethical computer use policy
    B. Anti-spam policy
    C. Information privacy policy
    D. Acceptable use policy

68. Which policy is it common practice for many businesses and educational facilities to require employees or students to sign before being granted a network ID?
    A. Information privacy policy
    B. Acceptable use policy
    C. Anti-spam policy
    D. Ethical computer use policy

69. What is one of the major problems with e-mail?
    A. Intellectual property
    B. Nonrepudiation
    C. User's expectation of privacy
    D. All of the above

70. Which of the following is part of the acceptable use policy stipulations?
    A. Not using the service as part of violating any law
    B. Not attempting to break the security of any computer network or user
    C. Not posting commercial messages to groups without prior permission
    D. All of the above

71. Which of the following is part of the acceptable use policy stipulations?
    A. Using the service to violate a law
    B. Posting commercial messages to groups without prior permission
    C. Performing nonrepudiation
    D. Not attempting to mail bomb a site

72. What is identity theft?
A. Is the forging of someone's identity for the purpose of fraud
B. Is monitoring emails
C. Is hacking in a computer system with the purpose of stealing information
D. Is buying illegal information from a hacker

73. Which policy details the extent to which e-mail messages may be read by others?
A. Acceptable use policy
B. E-mail privacy policy
C. Internet use policy
D. None of the above

74. Which of the following is not a part of the e-mail privacy policy stipulations?
A. It defines who legitimate e-mail users are
B. It explains the backup procedures
C. It describes the legitimate grounds for reading someone's e-mail
D. It informs people that the organization has full control over e-mail once it is transmitted outside the organization

75. Which of the following represents the estimated percentage that spam accounts for in an organizations' e-mail traffic?
A. 20 to 30 percent
B. 30 to 50 percent
C. 40 to 60 percent
D. None of the above

76. Which of the following describes information technology monitoring?
A. Tracking people's activities by such measures as number of keystrokes
B. Tracking people's activities by such measures as error rate
C. Tracking people's activities by such measures as number of transactions processed
D. All of the above

77. What is a program, when installed on a computer, records every keystroke and mouse click?
A. Key logger software
B. Spyware
C. Cookie
D. Adware

78. What is a hardware device that captures keystrokes on their journey from the keyboard to the motherboard?
A. Spyware
B. Hardware key logger
C. Cookie
D. Adware

79. Surprisingly, the biggest issue surrounding information security is not a people issue, but a technical issue.
True False

80. Information security is a broad term encompassing the protection of information from accidental or intentional misuse by persons inside or outside an organization.
True False

81. Insiders are illegitimate users who purposely or accidentally misuse their access to the environment to do business.
True False

82. Information security policies detail how an organization will implement the information security plan.
True False

83. Tokens are small electronic devices that change user passwords automatically.
True False

84. The Trojan-horse virus hides inside other software, usually as an attachment or a downloadable file.
True False

85. Confidentiality is the right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent.
True False

86. Opt-in implies that the customers will only be contacted if they agreed to receive promotions and marketing material.
True False

87. Ethical computer use policy contains general principles to guide computer user behaviour.
True False

88. Employee monitoring policies explicitly state how, when, and where the company monitors its employees.
True False

89. Information technology monitoring tracks people's activities by such measures as number of keystrokes, error rate, and number of transactions processed.
True False

90. How individuals behave toward each other, how they handle information, computer technologies, and information systems, are largely influenced by people's ethics.
True False

91. Ethical concerns over employee monitoring occurs when the monitoring is unprecedented or overly intrusive
True False

92. Breaches in information privacy occur when proper disclosure of personal information are made.
True False

93. Information privacy is about the prevention of collecting and sharing personal information.
True False

94. To facilitate information privacy, many countries have abolished legislation to protect the collection and sharing of personal information.
True False

95. The purpose of PIPEDA is to provide Europeans with a right of privacy with respect to how their personal information is collected, used, or disclosed by an organization.
True False

96. Employee monitoring policies explicitly state how, when, and where the company monitors its employees.
True False

97. _____ is software that comes hidden in free downloadable software and tracks online movements, mines the information stored on a computer, or uses a computer's CPU and storage for some task the user know nothing about.

_____

98. How individuals behave toward each other, how they handle information, computer technologies, and information systems, are largely influenced by people's _____.
_____

99. Ethical concerns over _____ monitoring occurs when the monitoring is unprecedented or overly intrusive
_____

100. To facilitate information privacy, many countries have established _____ to protect the collection and sharing of personal information.
_____

101. Breaches in information _____ occur when improper disclosure of personal information are made.
_____

102. The purpose of _____ is to provide Canadians with a right of privacy with respect to how their personal information is collected, used, or disclosed by an organization.
_____

103. Employee _____ policies explicitly state how, when, and where the company monitors its employees.
_____

104. Surprisingly, the biggest issue surrounding information security is not a technical issue, but a _____ issue.
_____

105. _____ security is a broad term encompassing the protection of information from accidental or intentional misuse by persons inside or outside an organization.
_____

106. Information security _____ identify the rules required to maintain information security.
_____

107. A(n) information security _____ details how an organization will implement the information security policies.
_____

108. Intrusion detection software (IDS) searches out patterns in information and network traffic to indicate _____ and quickly respond to prevent any harm.
_____

109. A(n) _____ is hardware and/or software that guards a private network by analyzing the information leaving and entering the network.
_____

110. Develop the information security policies is the _____ step for creating an information security plan.
_____

111. Obtain _____ support is the last step for creating an information security plan.
_____

112. Social engineering means using one's _____ skills to trick people into revealing access credentials or other information valuable to the attacker.
_____

113. _____ diving is a form of social engineering when a hacker looks through people's trash to find personal information.
_____

114._____ is a method for confirming users' identities.
_____

115.Tokens are small electronic devices that change user passwords _____.
_____

116.Smart card is a(n) _____ that is around the same size as a credit card, containing embedded technologies that can store information and small amounts of software to perform some limited processing.
_____

117._____ is the identification of a user based on a physical characteristic.
_____

118.Content filtering, _____, and firewalls are the three types of prevention and resistance technologies.
_____

119._____ scrambles information into an alternative form that requires a key or password to decrypt the information.
_____

120._____ filtering occurs when an organization uses software that filters content to prevent the transmission of unauthorized information.
_____

121.The most common type of defence within detection and response technologies is _____ software.
_____

122.Malicious code includes a variety of threats such as _____, worms, and Trojan horses.
_____

123._____ attack computer systems by transmitting a virus hoax, with a real virus attached.
_____

124.Spoofing is the forging of the _____ address on an e-mail so teat the e-mail message appears to come from someone other than the actual sender.
_____

125.A(n) _____ is a program or device that can monitor data traveling over a network.
_____

126._____ hat hackers work at the request of the system owners to find system vulnerabilities and plug the holes.
_____

127._____ hat hackers break into other people's computer systems and may just look around or may steal and destroy information.
_____

128._____ have philosophical and political reasons for breaking into systems and will often deface the Web site as a protest.
_____

129._____ kiddies find hacking code on the Internet and click-and-point their way into systems to cause damage or spread viruses.
_____

130._____ is a hacker with criminal intent.
_____

131._____ seek to cause harm to people or to destroy critical systems or information and use the Internet as a weapon of mass destruction.

_____

132._____ are people very knowledgeable about computers who use their knowledge to invade other people's computers.

_____

133.A(n) _____ is software written with malicious intent to cause annoyance or damage.

_____

134.A(n) _____ is a type of virus that spreads itself, not only from file to file, but also from computer to computer.

_____

135.Denial-of-service attack (DoS) _____ a Web site with so many requests for service that it slows down or crashes the site.

_____

136.Distributed denial-of-service attack (DDoS) attacks from multiple _____ that flood a Web site with so many requests for service that it slows down or crashes.

_____

137.The _____ of Death is a common type of DDoS and occurs when thousands of computers try to access a Web site at the same time, overloading it and shutting it down.

_____

138.Trojan-horse virus hides inside other _____, usually as an attachment or a downloadable file.

_____

139._____ programs are viruses that open a way into the network for future attacks.

_____

140._____ are the principles and standards that guide our behaviour toward other people.

_____

141._____ is the legal protection afforded an expression of an idea, such as a song, video game, and some types of proprietary documents.

_____

142.ePolicies are policies and procedures that address the ethical use of computers and Internet usage in the _____ environment.

_____

143._____ implies that contact will be made with only the people who had agreed to receive promotions and marketing materials.

_____

144.The _____ act restricts what information the federal government can collect.

_____

145.The pre-cursor to the Personal Information Protection and Electronic Documents Act (PIPEDA) was the _____ Act.

_____

146._____ is a US federal law established in 1998 that applies to the collection of personal information from American children who are under 13 years of age.

_____

147. The gist of the 10 Guiding Principles of PIPEDA for Organizations can be remembered as the 3Cs: Consent, Choice, and _____.
_____

148. A(n) _____ computer use policy contains general principles to guide computer user behaviour.
_____

149. A(n) _____ privacy policy contains general principles regarding information privacy.
_____

150. A(n) _____ use policy is a policy that a user must agree to follow in order to be provided access to a network or to the Internet.
_____

151. _____ is a contractual stipulation to ensure that e-business participants do not deny their online actions.
_____

152. A(n) _____ privacy policy details the extent to which e-mail messages may be read by others.
_____

153. A(n) _____ use policy contains general principles to guide the proper use of the Internet.
_____

154. _____ is unsolicited e-mail.
_____

155. Information technology _____ is tracking people's activities by such measures as number of keystrokes, error rate, and number of transactions processed.
_____

156. Key logger or key trapper software is a _____ that when installed on a computer, records every keystroke and mouse click.
_____

157. _____ key logger is a hardware device that captures keystrokes on their journey from the keyboard to the motherboard.
_____

158. _____ is software to generate ads that installs itself on a computer when a person downloads some other program from the Internet.
_____

159. Discuss the reasons why privacy issues lose trust for e-businesses.

160.Describe the relationship between information security policies and an information security plan.

161.Summarize the five steps to creating an information security plan.

162.List and describe the three primary security areas.

163.Describe authentication and the most secure type of authentication.

164.Describe the relationships and differences between hackers and viruses.

165.Describe the important ethical concepts stemming from information technology.

166. Explain the statement "information has no ethics."

167. Identify the differences between an ethical computer use policy and an acceptable computer use policy.

168. Describe the relationship between an e-mail privacy policy and in Internet use policy.

169. Summarize the different monitoring technologies and explain the importance of an employee monitoring policy

170. Explain how HIPAA protects individual's health records?

171. Describe the relationship between ethics and privacy.

09 Key

1. What is the recommended way to implement information security lines of defence?
(p. 292)
A. People first, technology second
B. Technology first, people second
C. None of the above
D. All of the above

An organization should implement information security lines of defence through people first and technology second.

Chapter - Chapter 09 #1
Gradable: automatic
Learning Outcome: 9.4
Level: Easy

2. Which term describes legitimate users who purposely or accidentally misuse their access to the environment and cause some kind of business-affecting incident?
(p. 292)
A. Hactivist
B. Social engineering
C. Insiders
D. Virus

This is the definition of insiders.

Chapter - Chapter 09 #2
Gradable: automatic
Learning Outcome: 9.4
Level: Easy

3. What identifies the rules required to maintain information security?
(p. 292)
A. Information security plan
B. Information security policies
C. Authentication
D. Biometrics

This is the definition of information security policies.

Chapter - Chapter 09 #3
Gradable: automatic
Learning Outcome: 9.4
Level: Easy

4. Which of the following is not one of the five steps for creating an information security plan?
(p. 292)
A. Develop the information security policies
B. Communicate the information security policies
C. Revise and test the information security policies
D. Test and reevaluate risks

Revise and test the information security policies is not part of the five steps for creating an information security plan.

Chapter - Chapter 09 #4
Gradable: automatic
Learning Outcome: 9.4
Level: Medium

5. What is social engineering?
(p. 292) **A.** Using one's social skills to trick people into revealing access credentials or other information valuable to the attacker
B. Legitimate users who purposely or accidentally misuse their access to the environment and cause some kind of business-affecting incident
C. Small electronic devices that change user passwords automatically
D. A method for confirming user's identities

This is the definition of social engineering.

Chapter - Chapter 09 #5
Gradable: automatic
Learning Outcome: 9.4
Level: Easy

6. Which of the following is not one of the top 10 questions managers should ask regarding information security?
(p. 293)
A. Is there clear accountability for information security in our organization?
B. How much is spent on information security and what is it being spent on?
C. What is the impact on the organization of a serious security incident?
D. How do we identify potential insiders?

How do we identify potential insiders is not one of the top ten questions managers should ask.

Chapter - Chapter 09 #6
Gradable: automatic
Learning Outcome: 9.4
Level: Hard

7. Which of the following is not one of the three primary information security areas?
(p. 294)
A. Authentication and authorization
B. Prevention and resistance
C. Detection and resistance
D. None of the above

Detection and resistance is not one of the three primary information security areas, it should be detection and response.

Chapter - Chapter 09 #7
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

8. What is a method for confirming users' identities?
(p. 294) **A.** Authentication
B. Prevention
C. Detection
D. Response

This is the definition of authentication.

Chapter - Chapter 09 #8
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

9. What is the most secure type of authentication?
(p. 294)
A. Something the user knows such as a user ID and password
B. Something the user has such as a smart card or token
C. Something that is part of the user such as a fingerprint or voice signature
D. Combination of all of the above

The most secure type of authentication involves a combination of all three.

Chapter - Chapter 09 #9
Gradable: automatic
Learning Outcome: 9.5
Level: Medium

10. What is a device that is around the same size as a credit card, containing embedded technologies that can store information and small amounts of software to perform some limited processing?
(p. 295)
A. Token
B. Password
C. Smart card
D. Biometrics

This is the definition of smart card.

Chapter - Chapter 09 #10
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

11. What is the identification of a user based on a physical characteristic, such as a fingerprint, iris, face, voice, or handwriting?
(p. 295)
A. Smart card
B. Token
C. Biometrics
D. Content filtering

This is the definition of biometrics.

Chapter - Chapter 09 #11
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

12. Which of the following is considered a type of biometrics?
(p. 295)
A. Voice
B. Face
C. Iris
D. All of the above

All of the above are considered biometrics.

Chapter - Chapter 09 #12
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

13. What is the most costly and intrusive form of authentication?
(p. 295)
A. Something the user knows such as a user ID and password
B. Something the user has such as a smart card or token
C. Something that is part of the user such as a fingerprint or voice signature
D. None of the above

Biometric authentication can be costly and intrusive.

Chapter - Chapter 09 #13
Gradable: automatic
Learning Outcome: 9.5
Level: Medium

14. Which of the following authentication methods is 100 percent accurate?
(p. 295)
A. Smart card
B. Fingerprint authentication
C. User ID
D. None of the above

None of the above authentication methods are 100 percent accurate.

Chapter - Chapter 09 #14
Gradable: automatic
Learning Outcome: 9.5
Level: Medium

15. What are the technologies available to help prevent and build resistance to attacks?
(p. 296)
A. Content filtering, encryption, firewalls
B. Content filtering, encryption, insiders
C. Encryption, firewalls, insiders
D. Firewalls, social engineering, encryption

Content filtering, encryption, and firewalls are technologies available to help prevent and build resistance to attacks.

Chapter - Chapter 09 #15
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

16. What occurs when an organization uses software that filters content to prevent the transmission of unauthorized information?
(p. 296)
A. Biometrics
B. Encryption
C. Firewalls
D. Content Filtering

Content filtering occurs when an organization uses software that filters content to prevent the transmission of unauthorized information.

Chapter - Chapter 09 #16
Gradable: automatic
Learning Outcome: 9.5
Level: Medium

17. What is spam?
(p. 286)
A. A type of encryption
B. A type of content filtering
C. A form of unsolicited e-mail
D. None of the above

This is the definition of spam.

Chapter - Chapter 09 #17
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

18. What is encryption?
(p. 296)
A. Occurs when an organization uses software that filters content to prevent the transmission of unauthorized information
B. Scrambles information into an alternative form that requires a key or password to decrypt the information
C. Hardware and/or software that guards a private network by analyzing the information leaving and entering the network
D. A form of unsolicited e-mail

This is the definition of encryption.

Chapter - Chapter 09 #18
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

19. Which of the following can be completed by encryption?
(p. 296)
A. Switch the order of characters
B. Replace characters with other characters
C. Use a mathematical formula to convert the information into some sort of code
D. All of the above

All of the above can be completed by encryption.

Chapter - Chapter 09 #19
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

20. Where do organizations typically place firewalls?
(p. 297)
A. Between a personal computer and the server
B. Between a personal computer and a printer
C. Between the server and the content filtering software
D. Between the server and the Internet

Firewalls are typically placed between a server and the Internet.

Chapter - Chapter 09 #20
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

21. Which of the following does a firewall perform?
(p. 290)
A. Examines each message that wants entrance to the network
B. Blocks messages without the correct markings from entering the network
C. Detects computers communicating with the Internet without approval
D. All of the above

A firewall can perform all of the above.

Chapter - Chapter 09 #21
Gradable: automatic
Learning Outcome: 9.5
Level: Medium

22. What includes a variety of threats such as viruses, worms, and Trojan horses?
(p. 299)
A. Malicious code
B. Hoaxes
C. Spoofing
D. Sniffer

This is the definition of malicious code.

Chapter - Chapter 09 #22
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

23. What is the forging of the return address on an e-mail so that the e-mail message appears to come from someone other than the actual sender?
(p. 299)
A. Malicious code
B. Hoaxes
C. Spoofing
D. Sniffer

This is the definition of spoofing.

Chapter - Chapter 09 #23
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

24. Which of the following is a program or device that can monitor data traveling over a network?
(p. 299)
A. Malicious code
B. Hoaxes
C. Spoofing
D. Sniffer

This is the definition of sniffer.

Chapter - Chapter 09 #24
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

25. What attacks computer systems by transmitting a virus hoax, with a real virus attached?
(p. 299)
A. Malicious code
B. Hoaxes
C. Spoofing
D. Sniffer

This is the definition of hoaxes.

Chapter - Chapter 09 #25
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

26. What is the most common type of defence within detection and response technologies?
(p. 297)
A. Malicious code
B. Token
C. User ID
D. Antivirus software

Antivirus software is the most common type of defence within detection and response technologies.

Chapter - Chapter 09 #26
Gradable: automatic
Learning Outcome: 9.5
Level: Medium

27. Who works at the request of the system owners to find system vulnerabilities and plug the holes?
(p. 298)
A. White-hat hackers
B. Black-hat hackers
C. Hactivists
D. Script kiddies

This is the definition of white-hat hackers.

Chapter - Chapter 09 #27
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

28. Who breaks into other people's computer systems and just looks around or steals and destroys information?
(p. 298)
A. White-hat hacker
B. Black-hat hacker
C. Hactivists
D. Script kiddies

This is the definition of black-hat hackers.

Chapter - Chapter 09 #28
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

29. *(p. 298)* Who finds hacking code on the Internet and click-and-points their way into systems to cause damage or spread viruses?
A. White-hat hacker
B. Black-hat hacker
C. Hactivists
D. Script kiddies

This is the definition of script kiddies.

Chapter - Chapter 09 #29
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

30. *(p. 298)* Who are hackers with criminal intent?
A. White-hat hacker
B. Black-hat hacker
C. Crackers
D. Cyberterrorists

This is the definition of crackers.

Chapter - Chapter 09 #30
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

31. *(p. 298)* Who are those who seek to cause harm to people or to destroy critical systems or information and use the Internet as a weapon of mass destruction?
A. White-hat hacker
B. Black-hat hacker
C. Crackers
D. Cyberterrorists

This is the definition of cyberterrorists.

Chapter - Chapter 09 #31
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

32. *(p. 298)* What is a type of virus that spreads itself, not just from file to file, but also from computer to computer?
A. Computer virus
B. Worm
C. Denial-of-service attack
D. None of the above

This is the definition of worm.

Chapter - Chapter 09 #32
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

33. What floods a Web site with so many requests for service that it slows down or crashes the site?
(p. 298)
A. Computer virus
B. Worm
C. Denial-of-service attack
D. None of the above

This is the definition of denial-of-service attack.

Chapter - Chapter 09 #33
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

34. Which is a virus that opens a way into the network for future attacks?
(p. 298)
A. Distributed denial-of-service attack
B. Worm
C. Denial-of-service attack
D. Backdoor programs

This is the definition of backdoor programs.

Chapter - Chapter 09 #34
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

35. If there is a security breech on your organizational information systems, which information security area is best suited to handle the breech?
(p. 299)
A. Authentication and authorization
B. Prevention and resistance
C. Detection and response
D. Detection and resistance

Detection and response technologies are used to handle security breeches.

Chapter - Chapter 09 #35
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

36. What are the principles and standards that guide our behaviour toward other people?
(p. 273)
A. Ethics
B. Intellectual property
C. Copyright
D. Fair Use Doctrine

This is the definition of ethics.

Chapter - Chapter 09 #36
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

37. What is intangible creative work that is embodied in physical form?
(p. 273)
A. Ethics
B. Intellectual property
C. Copyright
D. Fair Use Doctrine

This is the definition of intellectual property.

Chapter - Chapter 09 #37
Gradable: automatic
Learning Outcome: 9.1
Level: Medium

38. What is the legal protection afforded an expression of an idea, such as a song, video game, and some types of proprietary documents?
(p. 273)
A. Ethics
B. Intellectual property
C. Copyright
D. Fair Use Doctrine

This is the definition of copyright.

Chapter - Chapter 09 #38
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

39. What is it called when you may use copyrighted material in certain situations—for example, in the creation of new work or, within certain limits, for teaching purposes?
(p. 273)
A. Ethics
B. Intellectual property
C. Copyright
D. Fair dealing

This is the definition of fair dealing.

Chapter - Chapter 09 #39
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

40. What is the right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent?
(p. 273)
A. Fair Use Doctrine
B. Pirated software
C. Counterfeit software
D. Privacy

This is the definition of privacy.

Chapter - Chapter 09 #40
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

41. What is software that is manufactured to look like the real thing and sold as such?
(p. 273) A. Fair Use Doctrine
B. Pirated software
C. Counterfeit software
D. Privacy

This is the definition of counterfeit software.

Chapter - Chapter 09 #41
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

42. What is the unauthorized use, duplication, distribution, or sale of copyrighted software?
(p. 273) A. Fair Use Doctrine
B. Pirated software
C. Counterfeit software
D. Privacy

This is the definition of pirated software.

Chapter - Chapter 09 #42
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

43. What are the policies and procedures that address the ethical use of computers and Internet usage in the business environment?
(p. 283) A. Ethics
B. ePolicies
C. All of the above
D. None of the above

This is the definition of ePolicies.

Chapter - Chapter 09 #43
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

44. Which of the following describes privacy?
(p. 273) A. The assurance that messages and data are available only to those who are authorized to view them
B. Policies and procedures that address the ethical use of computers and Internet usage in the business environment
C The right to be left alone when you want to be, to have control over your own personal possessions, **.** and to not be observed without your consent
D. The principles and standards that guide our behaviour toward other people

This is the definition of privacy.

Chapter - Chapter 09 #44
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

45. Which of the following describes confidentiality?
(p. 273) **A.** The assurance that messages and information are available only to those who are authorized to view them
B. Policies and procedures that address the ethical use of computers and Internet usage in the business environment
C The right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent
D. The principles and standards that guide our behaviour toward other people

This is the definition of confidentiality.

Chapter - Chapter 09 #45
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

46. Which of the following describes ePolicies?
(p. 283) A. The assurance that messages and data are available only to those who are authorized to view them.
B. Policies and procedures that address the ethical use of computers and Internet usage in the business environment
C The right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent
D. The principles and standards that guide our behaviour toward other people

This is the definition of ePolicies.

Chapter - Chapter 09 #46
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

47. Which of the following is not considered an ePolicy?
(p. 283) A. Acceptable use policy
B. Internet use policy
C. Ethical computer use policy
D. None of the above

All of the above are ePolicies.

Chapter - Chapter 09 #47
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

48. Which of the following is an example of acting ethically?
(p. 274) A. Individuals copy, use, and distribute software
B. Employees search organizational databases for sensitive corporate and personal information.
C. Individuals hack into computer systems to steal proprietary information.
D. None of the above

None of the above are examples of acting ethically.

Chapter - Chapter 09 #48
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

49. Which of the following is not included in the four quadrants of ethical and legal behaviour?
(p. 274)
A. Legal behaviour and ethical behaviour
B. Illegal behaviour and ethical behaviour
C. Legal behaviour and unethical behaviour
D. None of the above

All of the above are contained in the four quadrants of ethical and legal behaviour.

Chapter - Chapter 09 #49
Gradable: automatic
Learning Outcome: 9.1
Level: Hard

50. What is the ideal type of decisions for people in an organization to make?
(p. 274)
A. Legal and ethical
B. Illegal and ethical
C. Legal and unethical
D. Illegal and unethical

The ideal goal for organizations is to make decisions within quadrant I that are both legal and ethical.

Chapter - Chapter 09 #50
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

51. What was the primary problem Saab encountered with one of its marketing companies?
(p. 274)
A. Contacted customers based on opt-out decision
B. Contacted customers based on opt-in decision
C. Contacted customers regardless of their opt-out or opt-in decision
D. Failed to contact any customers

One of Saab's marketing companies e-mailed all customers regardless of their opt-in decision.

Chapter - Chapter 09 #51
Gradable: automatic
Learning Outcome: 9.1
Level: Medium

52. What is a small file deposited on a hard drive by a Web site containing information about customers and their Web activities?
(p. 277)
A. Key logger
B. Hardware key logger
C. Cookie
D. Adware

This is the definition of cookie.

Chapter - Chapter 09 #52
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

53. Which of the following is an effect of employee monitoring?
(p. 276) **A.** Employee absenteeism is on the rise.
B. Job satisfaction is on the rise.
C. Psychological reactance is prevented.
D. All of the above.

The effects of employee monitoring are: absenteeism is on the rise, job satisfaction is lower, and psychological reactance is induced by electronic monitoring.

Chapter - Chapter 09 #53
Gradable: automatic
Learning Outcome: 9.1
Level: Hard

54. Canada's privacy laws follow very closely to the:
(p. 280) **A.** European model
B. US model
C. Bork model
D. None of the above

Canada's privacy laws follow very closely to the European model.

Chapter - Chapter 09 #54
Gradable: automatic
Learning Outcome: 9.2
Level: Hard

55. Which of the following is not one of the 10 Guiding principals of PIPEDA for organizations:
(p. 280) A. Accountability
B. Accuracy
C. Open access
D. Safeguards

Open access in not one of the 10 Guiding Principles.

Chapter - Chapter 09 #55
Gradable: automatic
Learning Outcome: 9.2
Level: Hard

56. Which of the following is/are covered by Canada's Privacy Act:
(p. 280) A. medical records
B. security clearances
C. tax records
D. All of the above

All of these were covered by The Privacy Act.

Chapter - Chapter 09 #56
Gradable: automatic
Learning Outcome: 9.2
Level: Hard

57. *(p. 283)* Which of the following is not one of the six principles for ethical information management according to CIO magazine?
A. Information is a valuable corporate asset and should be managed as such
B. The CIO is responsible for controlling access to and use of information
C. The CIO is responsible for preventing the inappropriate destruction of information
D. The CIO is responsible for how outsiders view and analyze corporate information

The CIO cannot be held responsible for how outsiders view and analyze corporate information, since the CIO has no responsibility over outsiders.

Chapter - Chapter 09 #57
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

58. *(p. 283)* What is the policy that contains general principles to guide computer user behaviour?
A. Information privacy policy
B. Acceptable use policy
C. Internet use policy
D. None of the above

The ethical computer use policy contains general principles to guide computer user behaviour.

Chapter - Chapter 09 #58
Gradable: automatic
Learning Outcome: 9.3
Level: Medium

59. *(p. 283)* Which policy ensures that the users know how to behave at work and that the organization has a published standard through which to deal with user infractions?
A. Information privacy policy
B. Acceptable use policy
C. Internet use policy
D. Ethical computer use policy

The ethical computer use policy must ensure that the users know how to behave and how infractions are handled.

Chapter - Chapter 09 #59
Gradable: automatic
Learning Outcome: 9.3
Level: Medium

60. *(p. 283)* According to the ethical computer use policy, users should be _____ of the rules and, by agreeing to use the system on that basis, _____ to abide by the rules.
A. Informed, collaborate
B. Consent, informed
C. Informed, consent
D. None of the above

Users should be informed of the computer rules and, by agreeing to use the system on that basis, consent to abide by the rules.

Chapter - Chapter 09 #60
Gradable: automatic
Learning Outcome: 9.3
Level: Medium

61. If an organization were to have only one policy, which one would it want?
(p. 283)
A. Information privacy policy
B. Acceptable use policy
C. Internet use policy
D. Ethical computer use policy

The ethical computer use policy is the starting point and umbrella for any other policies that the organization might establish.

Chapter - Chapter 09 #61
Gradable: automatic
Learning Outcome: 9.3
Level: Hard

62. Which policy contains general principles regarding information privacy?
(p. 283-284)
A. Information privacy policy
B. Acceptable use policy
C. Internet use policy
D. Anti-Spam policy

This is the definition of information privacy policy.

Chapter - Chapter 09 #62
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

63. Which of the following represents the classic example of unintentional information reuse?
(p. 284)
A. Phone number
B. Social Security number
C. Address
D. Driver's license number

The social security number is the classic example of unintentional information reuse in the United States.

Chapter - Chapter 09 #63
Gradable: automatic
Learning Outcome: 9.3
Level: Medium

64. What is one of the guidelines an organization can follow when creating an information privacy policy?
(p. 284)

A. Adoption and implementation of an anti-spam policy
B. Notice and disclosure
C. Choice and quality
D. None of the above

Notice and disclosure is the second guideline for creating an information privacy policy.

Chapter - Chapter 09 #64
Gradable: automatic
Learning Outcome: 9.3
Level: Medium

65. What is a policy that a user must agree to follow in order to be provided access to a network or to the Internet?
(p. 284)

A. Ethical computer use policy
B. Acceptable use policy
C. Nonrepudiation policy
D. None of the above

This is the definition of acceptable use policy.

Chapter - Chapter 09 #65
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

66. What is a contractual stipulation that ensures that e-business participants do not deny their online actions?
(p. 284)

A. Copyright
B. Fair use doctrine
C. Nonrepudiation
D. Intellectual property

This is the definition of nonrepudiation.

Chapter - Chapter 09 #66
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

67. Which policy typically contains a nonrepudiation clause?
(p. 284)

A. Ethical computer use policy
B. Anti-spam policy
C. Information privacy policy
D. Acceptable use policy

An AUP typically contains a nonrepudiation clause.

Chapter - Chapter 09 #67
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

68. Which policy is it common practice for many businesses and educational facilities to require employees or students to sign before being granted a network ID?
(p. 284)

A. Information privacy policy
B. Acceptable use policy
C. Anti-spam policy
D. Ethical computer use policy

It is common practice to sign an AUP before being granted a network ID.

Chapter - Chapter 09 #68
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

69. What is one of the major problems with e-mail?
(p. 285) A. Intellectual property
B. Nonrepudiation
C. User's expectation of privacy
D. All of the above

Users typically expect to receive the same type of privacy as is found in first-class mail.

Chapter - Chapter 09 #69
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

70. Which of the following is part of the acceptable use policy stipulations?
(p. 284) A. Not using the service as part of violating any law
B. Not attempting to break the security of any computer network or user
C. Not posting commercial messages to groups without prior permission
D. All of the above

All of the above are AUP stipulations.

Chapter - Chapter 09 #70
Gradable: automatic
Learning Outcome: 9.3
Level: Medium

71. Which of the following is part of the acceptable use policy stipulations?
(p. 284) A. Using the service to violate a law
B. Posting commercial messages to groups without prior permission
C. Performing nonrepudiation
D. Not attempting to mail bomb a site

Not attempting to mail bomb a site is part of the AUP stipulations.

Chapter - Chapter 09 #71
Gradable: automatic
Learning Outcome: 9.3
Level: Hard

72. What is identity theft?
(p. 277) **A.** Is the forging of someone's identity for the purpose of fraud
B. Is monitoring emails
C. Is hacking in a computer system with the purpose of stealing information
D. Is buying illegal information from a hacker

This is the definition of identity theft.

Chapter - Chapter 09 #72
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

73. Which policy details the extent to which e-mail messages may be read by others?
(p. 285)
A. Acceptable use policy
B. E-mail privacy policy
C. Internet use policy
D. None of the above

This is the definition of e-mail privacy policy.

Chapter - Chapter 09 #73
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

74. Which of the following is not a part of the e-mail privacy policy stipulations?
(p. 285)
A. It defines who legitimate e-mail users are
B. It explains the backup procedures
C. It describes the legitimate grounds for reading someone's e-mail
D. It informs people that the organization has full control over e-mail once it is transmitted outside the organization

The organization does not have any control over e-mail once it is transmitted outside of the organization.

Chapter - Chapter 09 #74
Gradable: automatic
Learning Outcome: 9.3
Level: Medium

75. Which of the following represents the estimated percentage that spam accounts for in an organizations' e-mail traffic?
(p. 286)
A. 20 to 30 percent
B. 30 to 50 percent
C. 40 to 60 percent
D. None of the above

Spam accounts for 40 to 60% of an organization's e-mail.

Chapter - Chapter 09 #75
Gradable: automatic
Learning Outcome: 9.1
Level: Medium

76. Which of the following describes information technology monitoring?
(p. 287)
A. Tracking people's activities by such measures as number of keystrokes
B. Tracking people's activities by such measures as error rate
C. Tracking people's activities by such measures as number of transactions processed
D. All of the above

This is the definition of information technology monitoring.

Chapter - Chapter 09 #76
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

77. What is a program, when installed on a computer, records every keystroke and mouse click?
(p. 277) **A.** Key logger software
B. Spyware
C. Cookie
D. Adware

This is the definition of key logger software.

Chapter - Chapter 09 #77
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

78. What is a hardware device that captures keystrokes on their journey from the keyboard to the
(p. 277) motherboard?
A. Spyware
B. Hardware key logger
C. Cookie
D. Adware

This is the definition of hardware key logger.

Chapter - Chapter 09 #78
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

79. Surprisingly, the biggest issue surrounding information security is not a people issue, but a technical
(p. 292) issue.
FALSE

Surprisingly, the biggest issue surrounding information security is not a technical issue, but a people issue.

Chapter - Chapter 09 #79
Gradable: automatic
Learning Outcome: 9.2
Level: Medium

80. Information security is a broad term encompassing the protection of information from accidental or
(p. 291) intentional misuse by persons inside or outside an organization.
TRUE

This is the definition of information security.

Chapter - Chapter 09 #80
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

81. Insiders are illegitimate users who purposely or accidentally misuse their access to the environment to
(p. 292) do business.
FALSE

Insiders are legitimate, not illegitimate, users who purposely or accidentally misuse their access to the environment and cause some kind of business-affecting incident.

Chapter - Chapter 09 #81
Gradable: automatic
Learning Outcome: 9.5
Level: Hard

82. Information security policies detail how an organization will implement the information security plan.
(p. 292)
FALSE

Information security plan details how an organization will implement the information security policies.

Chapter - Chapter 09 #82
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

83. Tokens are small electronic devices that change user passwords automatically.
(p. 295)
TRUE

This is the definition of token.

Chapter - Chapter 09 #83
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

84. The Trojan-horse virus hides inside other software, usually as an attachment or a downloadable file.
(p. 298)
TRUE

This is the definition for Trojan-horse virus.

Chapter - Chapter 09 #84
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

85. Confidentiality is the right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent.
(p. 273)
FALSE

Privacy is the right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent.

Chapter - Chapter 09 #85
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

86. Opt-in implies that the customers will only be contacted if they agreed to receive promotions and marketing material.
(p. 274)
TRUE

This is the definition of opt-in.

Chapter - Chapter 09 #86
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

87. Ethical computer use policy contains general principles to guide computer user behaviour.
(p. 283) **TRUE**

This is the definition of ethical computer use policy.

Chapter - Chapter 09 #87
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

88. Employee monitoring policies explicitly state how, when, and where the company monitors its
(p. 287) employees.
TRUE

This is the definition of employee monitoring policies.

Chapter - Chapter 09 #88
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

89. Information technology monitoring tracks people's activities by such measures as number of
(p. 287) keystrokes, error rate, and number of transactions processed.
TRUE

This is the definition of information technology monitoring.

Chapter - Chapter 09 #89
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

90. How individuals behave toward each other, how they handle information, computer technologies, and
(p. 273) information systems, are largely influenced by people's ethics.
TRUE

How individuals behave toward each other, how they handle information, computer technologies, and information systems, are largely influenced by people's ethics.

Chapter - Chapter 09 #90
Gradable: automatic
Learning Outcome: 9.1
Level: Medium

91. Ethical concerns over employee monitoring occurs when the monitoring is unprecedented or overly
(p. 275) intrusive
TRUE

Ethical concerns over employee monitoring occurs when the monitoring is unprecedented or overly intrusive

Chapter - Chapter 09 #91
Gradable: automatic
Learning Outcome: 9.1
Level: Medium

92. Breaches in information privacy occur when proper disclosure of personal information are made.
(p. 279) **FALSE**

Breaches in information privacy occur when improper disclosure of personal information are made.

Chapter - Chapter 09 #92
Gradable: automatic
Learning Outcome: 9.2
Level: Easy

93. Information privacy is about the prevention of collecting and sharing personal information.
(p. 279) **FALSE**

Information privacy is not about the prevention of collecting and sharing personal information.

Chapter - Chapter 09 #93
Gradable: automatic
Learning Outcome: 9.2
Level: Medium

94. To facilitate information privacy, many countries have abolished legislation to protect the collection and sharing of personal information.
(p. 279) **FALSE**

To facilitate information privacy, many countries have established legislation to protect the collection and sharing of personal information.

Chapter - Chapter 09 #94
Gradable: automatic
Learning Outcome: 9.2
Level: Medium

95. The purpose of PIPEDA is to provide Europeans with a right of privacy with respect to how their personal information is collected, used, or disclosed by an organization.
(p. 281) **FALSE**

The purpose of PIPEDA is to provide Canadians with a right of privacy with respect to how their personal information is collected, used, or disclosed by an organization.

Chapter - Chapter 09 #95
Gradable: automatic
Learning Outcome: 9.2
Level: Medium

96. Employee monitoring policies explicitly state how, when, and where the company monitors its employees.
(p. 287) **TRUE**

Employee monitoring policies explicitly state how, when, and where the company monitors its employees.

Chapter - Chapter 09 #96
Gradable: automatic
Learning Outcome: 9.3
Level: Medium

97. _____ is software that comes hidden in free downloadable software and tracks online movements, mines the information stored on a computer, or uses a computer's CPU and storage for some task the user know nothing about.
(p. 299) **Spyware**

Chapter - Chapter 09 #97
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

98. (p. 273) How individuals behave toward each other, how they handle information, computer technologies, and information systems, are largely influenced by people's _____.
ethics

Chapter - Chapter 09 #98
Gradable: automatic
Learning Outcome: 9.1
Level: Medium

99. (p. 275) Ethical concerns over _____ monitoring occurs when the monitoring is unprecedented or overly intrusive
employee

Chapter - Chapter 09 #99
Gradable: automatic
Learning Outcome: 9.2
Level: Medium

100. (p. 279) To facilitate information privacy, many countries have established _____ to protect the collection and sharing of personal information.
legislation

Chapter - Chapter 09 #100
Gradable: automatic
Learning Outcome: 9.2
Level: Medium

101. (p. 279) Breaches in information _____ occur when improper disclosure of personal information are made.
privacy

Chapter - Chapter 09 #101
Gradable: automatic
Learning Outcome: 9.2
Level: Medium

102. (p. 281) The purpose of _____ is to provide Canadians with a right of privacy with respect to how their personal information is collected, used, or disclosed by an organization.
PIPEDA

Chapter - Chapter 09 #102
Gradable: automatic
Learning Outcome: 9.2
Level: Medium

103. (p. 287) Employee _____ policies explicitly state how, when, and where the company monitors its employees.
monitoring

Chapter - Chapter 09 #103
Gradable: automatic
Learning Outcome: 9.3
Level: Medium

104. (p. 292) Surprisingly, the biggest issue surrounding information security is not a technical issue, but a _____ issue.
people

Chapter - Chapter 09 #104
Gradable: automatic
Learning Outcome: 9.4
Level: Medium

105. (p. 291) _____ security is a broad term encompassing the protection of information from accidental or intentional misuse by persons inside or outside an organization.
Information

Chapter - Chapter 09 #105
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

106. (p. 292) Information security _____ identify the rules required to maintain information security.
Policies

Chapter - Chapter 09 #106
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

107. A(n) information security _____ details how an organization will implement the information security policies.
(p. 292)
Plan

Chapter - Chapter 09 #107
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

108. Intrusion detection software (IDS) searches out patterns in information and network traffic to indicate _____ and quickly respond to prevent any harm.
(p. 293)
Attacks

Chapter - Chapter 09 #108
Gradable: automatic
Learning Outcome: 9.5
Level: Medium

109. A(n) _____ is hardware and/or software that guards a private network by analyzing the information leaving and entering the network.
(p. 297)
Firewall

Chapter - Chapter 09 #109
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

110. Develop the information security policies is the _____ step for creating an information security plan.
(p. 293)
First

Chapter - Chapter 09 #110
Gradable: automatic
Learning Outcome: 9.5
Level: Hard

111. Obtain _____ support is the last step for creating an information security plan.
(p. 293)
Stakeholder

Chapter - Chapter 09 #111
Gradable: automatic
Learning Outcome: 9.5
Level: Hard

112. Social engineering means using one's _____ skills to trick people into revealing access credentials or other information valuable to the attacker.
(p. 292)
Social

Chapter - Chapter 09 #112
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

113. _____ diving is a form of social engineering when a hacker looks through people's trash to find personal information.
(p. 292)
Dumpster

Chapter - Chapter 09 #113
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

114. _____ is a method for confirming users' identities.
(p. 294)
Authentication

Chapter - Chapter 09 #114
Gradable: automatic
Learning Outcome: 9.9
Level: Easy

115. Tokens are small electronic devices that change user passwords _____.
(p. 295)
Automatically

Chapter - Chapter 09 #115
Gradable: automatic
Learning Outcome: 9.9
Level: Medium

116. Smart card is a(n) _____ that is around the same size as a credit card, containing embedded technologies that can store information and small amounts of software to perform some limited processing. *(p. 295)*
Device

Chapter - Chapter 09 #116
Gradable: automatic
Learning Outcome: 9.9
Level: Hard

117. _____ is the identification of a user based on a physical characteristic. *(p. 295)*
Biometrics

Chapter - Chapter 09 #117
Gradable: automatic
Learning Outcome: 9.9
Level: Easy

118. Content filtering, _____, and firewalls are the three types of prevention and resistance technologies. *(p. 296)*
Encryption

Chapter - Chapter 09 #118
Gradable: automatic
Learning Outcome: 9.9
Level: Easy

119. _____ scrambles information into an alternative form that requires a key or password to decrypt the information. *(p. 296)*
Encryption

Chapter - Chapter 09 #119
Gradable: automatic
Learning Outcome: 9.9
Level: Easy

120. _____ filtering occurs when an organization uses software that filters content to prevent the transmission of unauthorized information. *(p. 296)*
Content

Chapter - Chapter 09 #120
Gradable: automatic
Learning Outcome: 9.9
Level: Easy

121. The most common type of defence within detection and response technologies is _____ software. *(p. 297)*
Antivirus

Chapter - Chapter 09 #121
Gradable: automatic
Learning Outcome: 9.5
Level: Medium

122. Malicious code includes a variety of threats such as _____, worms, and Trojan horses. *(p. 298)*
Viruses

Chapter - Chapter 09 #122
Gradable: automatic
Learning Outcome: 9.5
Level: Medium

123. _____ attack computer systems by transmitting a virus hoax, with a real virus attached. *(p. 299)*
Hoaxes

Chapter - Chapter 09 #123
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

124. Spoofing is the forging of the _____ address on an e-mail so teat the e-mail message appears to come from someone other than the actual sender. *(p. 299)*
Return

Chapter - Chapter 09 #124
Gradable: automatic
Learning Outcome: 9.5
Level: Medium

125. A(n) _____ is a program or device that can monitor data traveling over a network.
(p. 299) **Sniffer**

Chapter - Chapter 09 #125
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

126. _____ hat hackers work at the request of the system owners to find system vulnerabilities and
(p. 298) plug the holes.
White

Chapter - Chapter 09 #126
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

127. _____ hat hackers break into other people's computer systems and may just look around or
(p. 298) may steal and destroy information.
Black

Chapter - Chapter 09 #127
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

128. _____ have philosophical and political reasons for breaking into systems and will often deface
(p. 298) the Web site as a protest.
Hactivists

Chapter - Chapter 09 #128
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

129. _____ kiddies find hacking code on the Internet and click-and-point their way into
(p. 298) systems to cause damage or spread viruses.
Script

Chapter - Chapter 09 #129
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

130. _____ is a hacker with criminal intent.
(p. 298) **Cracker**

Chapter - Chapter 09 #130
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

131. _____ seek to cause harm to people or to destroy critical systems or information and use the
(p. 298) Internet as a weapon of mass destruction.
Cyberterrorists

Chapter - Chapter 09 #131
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

132. _____ are people very knowledgeable about computers who use their knowledge to invade other
(p. 298) people's computers.
Hackers

Chapter - Chapter 09 #132
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

133. A(n) _____ is software written with malicious intent to cause annoyance or damage.
(p. 298) **Virus**

Chapter - Chapter 09 #133
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

134. A(n) _____ is a type of virus that spreads itself, not only from file to file, but also from computer to computer. *(p. 298)*
Worm

Chapter - Chapter 09 #134
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

135. Denial-of-service attack (DoS) _____ a Web site with so many requests for service that it slows down or crashes the site. *(p. 298)*
Floods

Chapter - Chapter 09 #135
Gradable: automatic
Learning Outcome: 9.5
Level: Medium

136. Distributed denial-of-service attack (DDoS) attacks from multiple _____ that flood a Web site with so many requests for service that it slows down or crashes. *(p. 298)*
Computers

Chapter - Chapter 09 #136
Gradable: automatic
Learning Outcome: 9.5
Level: Medium

137. The _____ of Death is a common type of DDoS and occurs when thousands of computers try to access a Web site at the same time, overloading it and shutting it down. *(p. 298)*
Ping

Chapter - Chapter 09 #137
Gradable: automatic
Learning Outcome: 9.5
Level: Hard

138. Trojan-horse virus hides inside other _____, usually as an attachment or a downloadable file. *(p. 298)*
Software

Chapter - Chapter 09 #138
Gradable: automatic
Learning Outcome: 9.5
Level: Medium

139. _____ programs are viruses that open a way into the network for future attacks. *(p. 298)*
Backdoor

Chapter - Chapter 09 #139
Gradable: automatic
Learning Outcome: 9.5
Level: Easy

140. _____ are the principles and standards that guide our behaviour toward other people. *(p. 273)*
Ethics

Chapter - Chapter 09 #140
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

141. _____ is the legal protection afforded an expression of an idea, such as a song, video game, and some types of proprietary documents. *(p. 273)*
Copyright

Chapter - Chapter 09 #141
Gradable: automatic
Learning Outcome: 9.1
Level: Easy

142. ePolicies are policies and procedures that address the ethical use of computers and Internet usage in the _____ environment. *(p. 283)*
Business

Chapter - Chapter 09 #142
Gradable: automatic
Learning Outcome: 9.3
Level: Medium

143. _____ implies that contact will be made with only the people who had agreed to receive promotions and marketing materials. *(p. 274)*
Opt-in

Chapter - Chapter 09 #143
Gradable: automatic
Learning Outcome: 9.1
Level: Medium

144. The _____ act restricts what information the federal government can collect. *(p. 290)*
Privacy

Chapter - Chapter 09 #144
Gradable: automatic
Learning Outcome: 9.2
Level: Medium

145. The pre-cursor to the Personal Information Protection and Electronic Documents Act (PIPEDA) was the _____ Act. *(p. 290)*
Privacy

Chapter - Chapter 09 #145
Gradable: automatic
Learning Outcome: 9.2
Level: Medium

146. _____ is a US federal law established in 1998 that applies to the collection of personal information from American children who are under 13 years of age. *(p. 290)*
COPPA

Chapter - Chapter 09 #146
Gradable: automatic
Learning Outcome: 9.2
Level: Medium

147. The gist of the 10 Guiding Principles of PIPEDA for Organizations can be remembered as the 3Cs: Consent, Choice, and _____. *(p. 291)*
Control

Chapter - Chapter 09 #147
Gradable: automatic
Learning Outcome: 9.2
Level: Medium

148. A(n) _____ computer use policy contains general principles to guide computer user behaviour. *(p. 283)*
Ethical

Chapter - Chapter 09 #148
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

149. A(n) _____ privacy policy contains general principles regarding information privacy. *(p. 284)*
Information

Chapter - Chapter 09 #149
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

150. A(n) _____ use policy is a policy that a user must agree to follow in order to be provided access to a network or to the Internet. *(p. 284)*
Acceptable

Chapter - Chapter 09 #150
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

151. _____ is a contractual stipulation to ensure that e-business participants do not deny their online actions. *(p. 284)*
Nonrepudiation

Chapter - Chapter 09 #151
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

152. A(n) _____ privacy policy details the extent to which e-mail messages may be read by others. *(p. 285)*

E-mail

Chapter - Chapter 09 #152
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

153. A(n) _____ use policy contains general principles to guide the proper use of the Internet. *(p. 285)*

Internet

Chapter - Chapter 09 #153
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

154. _____ is unsolicited e-mail. *(p. 286)*

Spam

Chapter - Chapter 09 #154
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

155. Information technology _____ is tracking people's activities by such measures as number of keystrokes, error rate, and number of transactions processed. *(p. 277)*

Monitoring

Chapter - Chapter 09 #155
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

156. Key logger or key trapper software is a _____ that when installed on a computer, records every keystroke and mouse click. *(p. 277)*

Program

Chapter - Chapter 09 #156
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

157. _____ key logger is a hardware device that captures keystrokes on their journey from the keyboard to the motherboard. *(p. 277)*

Hardware

Chapter - Chapter 09 #157
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

158. _____ is software to generate ads that installs itself on a computer when a person downloads some other program from the Internet. *(p. 277)*

Adware

Chapter - Chapter 09 #158
Gradable: automatic
Learning Outcome: 9.3
Level: Easy

159. Discuss the reasons why privacy issues lose trust for e-businesses. *(p. 273)*

Loss of personal privacy is a top concern for Americans in the 21st century. Among Internet users, 37 percent would be "a lot" more inclined to purchase a product on a Web site that had a privacy policy. Privacy/security is the #1 factor that would convert Internet researchers into Internet buyers.

Chapter - Chapter 09 #159
Gradable: manual
Learning Outcome: 9.1
Level: Medium

160. Describe the relationship between information security policies and an information security plan.
(p. 292)

The information security plan details how the organization will implement the information security policies. Information security policies identify the rules required to maintain information security.

Chapter - Chapter 09 #160
Gradable: manual
Learning Outcome: 9.4
Level: Easy

161. Summarize the five steps to creating an information security plan.
(p. 292)

Develop the information security policies, (2) Communicate the information security policies, (3) Identify critical information assets and risks, (4) Test and reevaluate risks, (5) Obtain stakeholder support

Chapter - Chapter 09 #161
Gradable: manual
Learning Outcome: 9.4
Level: Easy

162. List and describe the three primary security areas.
(p. 294)

(1) Authentication and authorization Something the user knows such as a user ID and password, something the user has such as a smart card or token, something that is part of the user such as fingerprint or voice signature, (2) Prevention and resistance-Content filtering, encryption, firewalls, (3) Detection and response-Antivirus software

Chapter - Chapter 09 #162
Gradable: manual
Learning Outcome: 9.5
Level: Medium

163. Describe authentication and the most secure type of authentication.
(p. 294)

Authentication is a method for confirming user's identities. The most secure type of authentication involves a combination of the following: something the user knows such as a user ID and password, something the user has such as a smart card or token, something that is part of the user such as fingerprint or voice signature.

Chapter - Chapter 09 #163
Gradable: manual
Learning Outcome: 9.5
Level: Medium

164. Describe the relationships and differences between hackers and viruses.
(p. 298)

Hackers are people very knowledgeable about computers who use their knowledge to invade other people's computers. Viruses are software written with malicious intent to cause annoyance or damage.

Chapter - Chapter 09 #164
Gradable: manual
Learning Outcome: 9.5
Level: Easy

165. Describe the important ethical concepts stemming from information technology.
(p. 273)

Intellectual property-intangible creative work that is embodied in physical form. Copyright-the legal protection afforded an expression of an idea, such as a song, video game, and some types of proprietary documents. Fair use doctrine-it is legal to use copyrighted material in certain situations. Pirated software-the unauthorized use, duplication, distribution, or sale of copyrighted software. Counterfeit software-manufactured to look like the real thing and sold as such.

Chapter - Chapter 09 #165
Gradable: manual
Learning Outcome: 9.1
Level: Easy

166. Explain the statement "information has no ethics."
(p. 274)

Information has no ethics. Information does not care how it is used. Information will not stop itself from sending spam, viruses, or highly-sensitive information. Information cannot delete or preserve itself. For these reasons it falls on the shoulders of those who lord over the information to develop ethical guidelines on how to mange it

Chapter - Chapter 09 #166
Gradable: manual
Learning Outcome: 9.1
Level: Easy

167. Identify the differences between an ethical computer use policy and an acceptable computer use policy.
(p. 284)

Ethical computer use policy-contains general principles to guide computer user behaviour. The ethical computer user policy ensures all users are informed of the rules and, by agreeing to use the system on that basis, consent to abide by the rules. Acceptable use policy (AUP)-a policy that a user must agree to follow in order to be provided access to a network or to the Internet. An AUP usually contains a nonrepudiation clause: Nonrepudiation-a contractual stipulation to ensure that e-business participants do not deny (repudiate) their online actions.

Chapter - Chapter 09 #167
Gradable: manual
Learning Outcome: 9.3
Level: Medium

168. Describe the relationship between an e-mail privacy policy and in Internet use policy.
(p. 285)

Organizations can mitigate the risks of e-mail and instant messaging communication tools by implementing and adhering to an e-mail privacy policy. E-mail privacy policy details the extent to which e-mail message may be read by others. An Internet use policy contains general principles to guide the proper use of the Internet. The Internet use policy covers all acts taking place on the Internet, whereas the e-mail privacy policy simply includes e-mail.

Chapter - Chapter 09 #168
Gradable: manual
Learning Outcome: 9.3
Level: Easy

169. Summarize the different monitoring technologies and explain the importance of an employee monitoring policy
(p. 275)

Different monitoring technologies include (1) Key logger, or key trapper software-records keystrokes and mouse clicks, (2) Hardware key logger-capture keystrokes from the keyboard to the motherboard, (3) Cookie-small file deposited on a hard drive by a Web site containing information about customers and their Web activities, (4) Adware-generates self installing ads, (5) Spyware-hidden software that tracks online movements, (6) Web log-consists of one line of information for every visitor to a Web site, (7) Clickstream-records information about a customer during a Web surfing session. Employee monitoring policies explicitly state how, when, and where the company monitors its employees.

Chapter - Chapter 09 #169
Gradable: manual
Learning Outcome: 9.3
Level: Easy

170. Explain how HIPAA protects individual's health records?
(p. 280)

HIPAA is the Health Insurance Portability and Accountability Act. HIPAA helps protect the privacy and security of personal health records by requiring all health care organizations to develop, implement, and maintain appropriate security measures when sending electronic health information.

Chapter - Chapter 09 #170
Gradable: manual
Learning Outcome: 9.3
Level: Hard

171. Describe the relationship between ethics and privacy.
(p. 265)

Ethics are the principles and standards that guide our behaviour toward other people
Privacy is the right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent. Privacy is an ethical issue.

Chapter - Chapter 09 #171
Gradable: manual
Learning Outcome: 9.1
Level: Easy

09 Summary

Category	*# of Questions*
Chapter - Chapter 09	171
Gradable: automatic	158
Gradable: manual	13
Learning Outcome: 9.1	30
Learning Outcome: 9.2	16
Learning Outcome: 9.3	44
Learning Outcome: 9.4	9
Learning Outcome: 9.5	65
Learning Outcome: 9.9	7
Level: Easy	108
Level: Hard	14
Level: Medium	49