https://selldocx.com/products

Chapter 02 - Secure Information Systems

/test-bank-principles-of-information-systems-14e-reynolds

True / False

1. As the complexity of a network increases, the possibility of security breaches decreases.

a. True
b. False

ANSWER: False

RATIONALE: The computing environment continues to increase in complexity every day and soon will include billions of communicating devices. The number of possible entry points to a network expands continually as more devices are added, further increasing the possibility of security breaches.

FEEDBACK:
Correct The computing environment continues to increase in complexity every day and soon will include billions of communicating devices. The number of possible entry points to a network expands continually as more devices are added, further increasing the possibility of security breaches.
Incorrect The computing environment continues to increase in complexity every day and soon will include billions of communicating devices. The number of possible entry points to a network expands continually as more devices are added, further increasing the possibility of security breaches.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Why Computer Incidents Are So Prevalent
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.1 - State four reasons why computer incidents have become so prevalent.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/15/2019 4:26 PM

2. An attack that takes place before the security community and/or software developers become aware of and fix a security vulnerability is called a zero-day attack.

a. True
b. False

ANSWER: True

RATIONALE: Of special concern is a zero-day attack, which is an attack that takes place before the security community becomes aware of and fixes a security vulnerability. Zero-day attacks are rare—just eight were identified in 2016 and 49 were identified in 2017.

FEEDBACK:
Correct Of special concern is a zero-day attack, which is an attack that takes place before the security community becomes aware of and fixes a security vulnerability. Zero-day attacks are rare—just eight were identified in 2016 and 49 were identified in 2017.
Incorrect Of special concern is a zero-day attack, which is an attack that takes place before the security community becomes aware of and fixes a security vulnerability. Zero-day attacks are rare—just eight were identified in 2016 and 49 were identified in 2017.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Why Computer Incidents Are So Prevalent
QUESTION TYPE: True / False

Copyright Cengage Learning. Powered by Cognero.

HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.1 - State four reasons why computer incidents have become so prevalent.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/20/2019 4:00 PM

3. Discovery of a vulnerability in a software program can potentially be sold to the government.

a. True
b. False

ANSWER: True
RATIONALE: While one would hope that the discoverer of a zero-day vulnerability would immediately inform the original software manufacturer so that a fix could be created for the problem, that is not always the case. In some cases, this knowledge is instead sold on the black market to cyberterrorists, governments, or large organizations that may then use it to launch their own cyberattacks.
FEEDBACK:
Correct In some cases, knowledge of a zero-day vulnerability is sold on the black market to cyberterrorists, governments, or large organizations that may then use it to launch their own cyberattacks.
Incorrect In some cases, knowledge of a zero-day vulnerability is sold on the black market to cyberterrorists, governments, or large organizations that may then use it to launch their own cyberattacks.
POINTS: 1
DIFFICULTY: Easy
REFERENCES: Why Computer Incidents Are So Prevalent
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.1 - State four reasons why computer incidents have become so prevalent.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/20/2019 4:08 PM

4. You see a deceptive pop-up that says that your computer is infected, and then you are forced to visit a website where you pay for "computer clean-up" in order to access data from your hard drive. You have just become a victim of ransomware.

a. True
b. False

ANSWER: True
RATIONALE: Ransomware is malware that stops you from using your computer or accessing the data on your computer until you meet certain demands, such as paying a ransom or, in some cases, sending compromising photos to the attacker.
FEEDBACK:
Correct Ransomware is malware that stops you from using your computer or accessing the data on your computer until you meet certain demands, such as paying a ransom or, in some

Copyright Cengage Learning. Powered by Cognero.

cases, sending compromising photos to the attacker.

Incorrect Ransomware is malware that stops you from using your computer or accessing the data on your computer until you meet certain demands, such as paying a ransom or, in some cases, sending compromising photos to the attacker.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Cyberattacks That Pose Serious Threats
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.5 - Identify five cyberthreats that pose a serious threat for organizations.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/20/2019 4:14 PM

5. Even legitimate organizations sometimes use worms, unsolicited email messages sent to large numbers of people, to promote their products.

a. True
b. False

ANSWER: False
RATIONALE: There are numerous types of attack vectors. One is spam, the use of email systems to send unsolicited email to large numbers of people. Another is a worm, a harmful program that resides in the active memory of the computer and duplicates itself.
FEEDBACK:
Correct A worm is a harmful program that resides in the active memory of the computer and duplicates itself.
Incorrect A worm is a harmful program that resides in the active memory of the computer and duplicates itself.
POINTS: 1
DIFFICULTY: Easy
REFERENCES: Types of Attack Vectors
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.4 - Identify at least three commonly used attack vectors.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/20/2019 4:24 PM

6. A zombie computer sends requests for access to a target site again and again.

a. True
b. False

ANSWER: True

Copyright Cengage Learning. Powered by Cognero.

RATIONALE: In a DDoS attack, a tiny program is downloaded surreptitiously from the attacker's computer to dozens, hundreds, or even thousands of computers all over the world. The term botnet is used to describe a large group of such computers, which are controlled from one or more remote locations by hackers, without the knowledge or consent of their legitimate owners. Based on a command by the attacker or at a preset time, the botnet computers (called zombies) go into action, each sending a simple request for access to the target site again and again—dozens of times per second.

FEEDBACK:
- *Correct* In a DDoS attack, botnet computers (called zombies) go into action, each sending a simple request for access to the target site again and again—dozens of times per second.
- *Incorrect* In a DDoS attack, botnet computers (called zombies) go into action, each sending a simple request for access to the target site again and again—dozens of times per second.

POINTS: 1

DIFFICULTY: Easy

REFERENCES: Cyberattacks That Pose Serious Threats

QUESTION TYPE: True / False

HAS VARIABLES: False

LEARNING OBJECTIVES: POIS.14e.2.5 - Identify five cyberthreats that pose a serious threat for organizations.

NATIONAL STANDARDS: United States - BUSPROG: Technology

KEYWORDS: Bloom's: Remember

DATE CREATED: 11/19/2019 5:58 PM

DATE MODIFIED: 12/20/2019 4:32 PM

7. When you receive a text message that there is a problem with your bank account and you are required you to click on a link to submit some information, you are likely facing a vishing attack.

a. True

b. False

ANSWER: False

RATIONALE: There are numerous types of attack vectors. One is phishing, the act of fraudulently using email to try to get the recipient to reveal personal data. Smishing is a variation of phishing that involves the use of texting. Vishing is similar to smishing except that the victims receive a voice mail message telling them to call a phone number or access a Web site.

FEEDBACK:
- *Correct* Smishing is a variation of phishing that involves the use of texting. Vishing is similar to smishing except that the victims receive a voice mail message telling them to call a phone number or access a Web site.
- *Incorrect* Smishing is a variation of phishing that involves the use of texting. Vishing is similar to smishing except that the victims receive a voice mail message telling them to call a phone number or access a Web site.

POINTS: 1

DIFFICULTY: Easy

REFERENCES: Types of Attack Vectors

QUESTION TYPE: True / False

HAS VARIABLES: False

LEARNING OBJECTIVES: POIS.14e.2.4 - Identify at least three commonly used attack vectors.

NATIONAL STANDARDS: United States - BUSPROG: Technology

Copyright Cengage Learning. Powered by Cognero.

ARDS:
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/20/2019 4:36 PM

8. You discover that an unknown party has gained administrator-level access to your computer, but the programs allowing this invasion are not visible to the legitimate system administrators. You have probably been hit by a rootkit.

a. True
b. False

ANSWER: True
RATIONALE: There are numerous types of attack vectors. One is a rootkit, a set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge. Once installed, the attacker can gain full control of the system and even obscure the presence of the rootkit from legitimate system administrators.
FEEDBACK:
Correct A rootkit is a set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge. Once installed, the attacker can gain full control of the system and even obscure the presence of the rootkit from legitimate system administrators.
Incorrect A rootkit is a set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge. Once installed, the attacker can gain full control of the system and even obscure the presence of the rootkit from legitimate system administrators.
POINTS: 1
DIFFICULTY: Moderate
REFERENCES: Types of Attack Vectors
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.4 - Identify at least three commonly used attack vectors.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/20/2019 4:41 PM

9. Downloading games from unknown websites can be risky. The software may be a Trojan horse.

a. True
b. False

ANSWER: True
RATIONALE: There are numerous types of attack vectors. One is a Trojan horse, a seemingly harmless program in which malicious code is hidden. A victim on the receiving end of a Trojan horse is usually tricked into opening it because it appears to be useful software from a legitimate source.
FEEDBACK:
Correct A Trojan horse is a seemingly harmless program in which malicious code is hidden. A victim on the receiving end of a Trojan horse is usually tricked into opening it because it appears to be useful software from a legitimate source.
Incorrect A Trojan horse is a seemingly harmless program in which malicious code is hidden. A victim on the receiving end of a Trojan horse is usually tricked into opening it because it appears to be useful software from a legitimate source.

Copyright Cengage Learning. Powered by Cognero.

POINTS: 1
DIFFICULTY: Moderate
REFERENCES: Types of Attack Vectors
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.4 - Identify at least three commonly used attack vectors.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/20/2019 4:44 PM

10. You work at a call center of a large bank, where you answer credit card services-related questions from customers. Lately, you have noticed an increased number of customers enquiring whether your organization initiated a call about their account. There might be a vishing scam in progress.

a. True
b. False

ANSWER: True
RATIONALE: There are numerous types of attack vectors. One is vishing, in which victims receive a voice mail message telling them to call a phone number or access a Web site. This is a way to fraudulently try to get the recipient to reveal personal data.
FEEDBACK:
Correct In vishing, victims receive a voice mail message telling them to call a phone number or access a Web site.
Incorrect In vishing, victims receive a voice mail message telling them to call a phone number or access a Web site.
POINTS: 1
DIFFICULTY: Moderate
REFERENCES: Types of Attack Vectors
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.4 - Identify at least three commonly used attack vectors.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/20/2019 4:54 PM

11. Transmitting a program, code, or command that causes harm to a computer is a crime.

a. True
b. False

ANSWER: True
RATIONALE: Over the years, the United States Congress has enacted multiple laws to help prosecute those responsible for computer-related crime. The Computer Fraud and Abuse Act addresses fraud and related activities in association with computers, including transmitting a program, code, or

command that causes harm to a computer.

FEEDBACK:
Correct The Computer Fraud and Abuse Act addresses fraud and related activities in association with computers, including transmitting a program, code, or command that causes harm to a computer.
Incorrect The Computer Fraud and Abuse Act addresses fraud and related activities in association with computers, including transmitting a program, code, or command that causes harm to a computer.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Federal Laws for Prosecuting Computer Attacks
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.7 - Identify five federal laws that address computer crime.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/22/2019 5:47 PM

12. Those convicted of cyberterrorism are subject to a prison term of 6 months to 1 year.

a. True
b. False

ANSWER: False
RATIONALE: Those convicted of cyberterrorism are subject to a prison term of 5–20 years.
FEEDBACK:
Correct Those convicted of cyberterrorism are subject to a prison term of 5–20 years.
Incorrect Those convicted of cyberterrorism are subject to a prison term of 5–20 years.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Federal Laws for Prosecuting Computer Attacks
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.7 - Identify five federal laws that address computer crime.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/22/2019 5:53 PM

13. A strong security program begins by assessing the backgrounds of the employees in the organization.

a. True
b. False

ANSWER: False
RATIONALE: Confidentiality, integrity, and availability are referred to as the CIA security triad. Implementing CIA begins at the organizational level with the definition of an overall security strategy, performance of a risk assessment, laying out plans for disaster recovery, setting security policies, conducting security audits, ensuring regulatory standards compliance, and creating a security

Copyright Cengage Learning. Powered by Cognero.

dashboard.

FEEDBACK:
Correct Implementing CIA begins at the organizational level with the definition of an overall security strategy, performance of a risk assessment, laying out plans for disaster recovery, setting security policies, conducting security audits, ensuring regulatory standards compliance, and creating a security dashboard.
Incorrect Implementing CIA begins at the organizational level with the definition of an overall security strategy, performance of a risk assessment, laying out plans for disaster recovery, setting security policies, conducting security audits, ensuring regulatory standards compliance, and creating a security dashboard.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the Organizational Level
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization, network, application, and end user levels to safeguard against cyberattacks.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/22/2019 5:58 PM

14. Default usernames and passwords should always be changed.

a. True
b. False

ANSWER: True
RATIONALE: System administrators must be vigilant about changing the default usernames and passwords for specific devices when they are added to an organization's network. Cybercriminals and others looking to access the networks of various organizations can easily find information online regarding the default username and password combinations for many vendors' products.

FEEDBACK:
Correct System administrators must be vigilant about changing the default usernames and passwords for specific devices when they are added to an organization's network.
Incorrect System administrators must be vigilant about changing the default usernames and passwords for specific devices when they are added to an organization's network.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the Organizational Level
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization, network, application, and end user levels to safeguard against cyberattacks.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/22/2019 6:00 PM

Copyright Cengage Learning. Powered by Cognero.

15. An employee who is about to be laid off by his organization sends threatening emails to his boss, stating that he is going to delete sensitive data. This employee can be charged under the Computer Fraud and Abuse Act.

a. True
b. False

ANSWER: True
RATIONALE: The Computer Fraud and Abuse Act addresses fraud and related activities in association with computers, including accessing a computer without authorization or exceeding authorized access and threatening to cause damage to a protected computer.
FEEDBACK:
Correct The Computer Fraud and Abuse Act addresses fraud and related activities in association with computers, including accessing a computer without authorization or exceeding authorized access and threatening to cause damage to a protected computer.
Incorrect The Computer Fraud and Abuse Act addresses fraud and related activities in association with computers, including accessing a computer without authorization or exceeding authorized access and threatening to cause damage to a protected computer.
POINTS: 1
DIFFICULTY: Moderate
REFERENCES: Federal Laws for Prosecuting Computer Attacks
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.7 - Identify five federal laws that address computer crime.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/22/2019 6:04 PM

16. A "virus signature" contains the email address of the virus developer.

a. True
b. False

ANSWER: False
RATIONALE: Antivirus software should be installed on each user's personal computer to scan a computer's memory and disk drives regularly for viruses. Antivirus software scans for a specific sequence of bytes, known as a virus signature, that indicates the presence of a specific virus.
FEEDBACK:
Correct Antivirus software scans for a specific sequence of bytes, known as a virus signature, that indicates the presence of a specific virus.
Incorrect Antivirus software scans for a specific sequence of bytes, known as a virus signature, that indicates the presence of a specific virus.
POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the End-User Level
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization, network, application, and end user levels to safeguard against cyberattacks.
NATIONAL STANDARDS: United States - BUSPROG: Technology

Copyright Cengage Learning. Powered by Cognero.

KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/22/2019 6:07 PM

17. Any Internet traffic that is not explicitly permitted into the internal network is denied entry through a firewall.

a. True
b. False

ANSWER: True
RATIONALE: A firewall is a system of software, hardware, or a combination of both that stands guard between an organization's internal network and the Internet, and limits network access based on the organization's access policy. Any Internet traffic that is not explicitly permitted into the internal network is denied entry through a firewall.
FEEDBACK:
Correct Any Internet traffic that is not explicitly permitted into the internal network is denied entry through a firewall.
Incorrect Any Internet traffic that is not explicitly permitted into the internal network is denied entry through a firewall.
POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the Network Level
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization, network, application, and end user levels to safeguard against cyberattacks.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/22/2019 6:09 PM

18. Scanning a computer's hard drive for viruses is essential, but scanning live memory is only important in certain situations.

a. True
b. False

ANSWER: False
RATIONALE: Antivirus software should be installed on each user's personal computer to scan a computer's memory and disk drives regularly for viruses. Good antivirus software checks vital system files when the system is booted up, monitors the system continuously for virus-like activity, scans disks, scans memory when a program is run, checks programs when they are downloaded, and scans email attachments before they are opened.
FEEDBACK:
Correct Antivirus software should be installed on each user's personal computer to scan a computer's memory and disk drives regularly for viruses.
Incorrect Antivirus software should be installed on each user's personal computer to scan a computer's memory and disk drives regularly for viruses.
POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the End-User Level
QUESTION TYPE: True / False

Copyright Cengage Learning. Powered by Cognero.

HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization, network, application, and end user levels to safeguard against cyberattacks.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/22/2019 6:15 PM

19. When a computer security incident occurs, it is recommended that the organization NOT reveal all they know in public forums.

a. True
b. False

ANSWER: True
RATIONALE: A key element of any response plan is to define who to notify and who not to notify in the event of a computer security incident. Most security experts recommend against giving out specific information about a compromise in public forums, such as news reports, conferences, professional meetings, and online discussion groups.
FEEDBACK:
Correct Most security experts recommend against giving out specific information about a compromise in public forums, such as news reports, conferences, professional meetings, and online discussion groups.
Incorrect Most security experts recommend against giving out specific information about a compromise in public forums, such as news reports, conferences, professional meetings, and online discussion groups.
POINTS: 1
DIFFICULTY: Easy
REFERENCES: Response
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.11 - Describe five actions an organization must take in response to a successful cyberattack.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/22/2019 6:18 PM

20. There are laws that require businesses to prove that their data are secure.

a. True
b. False

ANSWER: True
RATIONALE: Keeping up with computer criminals—and with new laws and regulations—can be daunting for organizations. Laws such as HIPAA, Sarbanes-Oxley, and the USA Patriot Act require businesses to prove that they are securing their data.
FEEDBACK:
Correct Laws such as HIPAA, Sarbanes-Oxley, and the USA Patriot Act require businesses to prove that they are securing their data.
Incorrect Laws such as HIPAA, Sarbanes-Oxley, and the USA Patriot Act require businesses to

Copyright Cengage Learning. Powered by Cognero.

prove that they are securing their data.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Using a Managed Security Service Provider (MSSP)
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.12 - Describe the role of a managed security service provider.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/22/2019 6:26 PM

21. It is considered ethical for an organization to conceal information about a data loss event to avoid bad publicity and loss of customers.

a. True
b. False

ANSWER: False
RATIONALE: A critical ethical decision that must be made is what to tell customers and others whose personal data may have been compromised by a computer incident. Many organizations are tempted to conceal such information for fear of bad publicity and loss of customers. Because such inaction is perceived by many to be unethical and harmful, several state and federal laws have been passed to force organizations to reveal when customer data has been breached.
FEEDBACK:
Correct Many organizations are tempted to conceal information regarding whose personal data may have been compromised by a computer incident for fear of bad publicity and loss of customers, but such inaction is perceived by many to be unethical and harmful.
Incorrect Many organizations are tempted to conceal information regarding whose personal data may have been compromised by a computer incident for fear of bad publicity and loss of customers, but such inaction is perceived by many to be unethical and harmful.
POINTS: 1
DIFFICULTY: Easy
REFERENCES: Response
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.11 - Describe five actions an organization must take in response to a successful cyberattack.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 9:57 AM

22. If an attack is dangerous enough, it may warrant shutting down or disconnecting critical systems from the network.

a. True
b. False

Copyright Cengage Learning. Powered by Cognero.

ANSWER: True

RATIONALE: Often, it is necessary to act quickly to contain an attack and to keep a bad situation from becoming even worse. The incident response plan should clearly define the process for deciding if an attack is dangerous enough to warrant shutting down or disconnecting critical systems from the network.

FEEDBACK:
- *Correct* Often, it is necessary to act quickly to contain an attack and to keep a bad situation from becoming even worse. The incident response plan should clearly define the process for deciding if an attack is dangerous enough to warrant shutting down or disconnecting critical systems from the network.
- *Incorrect* Often, it is necessary to act quickly to contain an attack and to keep a bad situation from becoming even worse. The incident response plan should clearly define the process for deciding if an attack is dangerous enough to warrant shutting down or disconnecting critical systems from the network.

POINTS: 1

DIFFICULTY: Easy

REFERENCES: Response

QUESTION TYPE: True / False

HAS VARIABLES: False

LEARNING OBJECTIVES: POIS.14e.2.11 - Describe five actions an organization must take in response to a successful cyberattack.

NATIONAL STANDARDS: United States - BUSPROG: Technology

KEYWORDS: Bloom's: Remember

DATE CREATED: 11/19/2019 5:58 PM

DATE MODIFIED: 12/26/2019 10:01 AM

23. Suppose your computer network was compromised in a large-scale virus attack last Thursday. Most of the data files were corrupted beyond repair. The last data backup was done the Sunday before the virus attack. This means your company has an adequate backup process in place.

a. True
b. False

ANSWER: False

RATIONALE: It is imperative to back up critical applications and data regularly. Many organizations, however, have implemented inadequate backup processes and found that they could not fully restore original data after a security incident. All backups should be created with enough frequency to enable a full and quick restoration of data if an attack destroys the original, and this process must be tested to confirm that it works.

FEEDBACK:
- *Correct* All backups should be created with enough frequency to enable a full and quick restoration of data if an attack destroys the original, and this process must be tested to confirm that it works.
- *Incorrect* All backups should be created with enough frequency to enable a full and quick restoration of data if an attack destroys the original, and this process must be tested to confirm that it works.

POINTS: 1

DIFFICULTY: Moderate

REFERENCES: Response

QUESTION TYPE: True / False

HAS VARIABLES: False

LEARNING OBJECTIVES: POIS.14e.2.11 - Describe five actions an organization must take in response to a

Copyright Cengage Learning. Powered by Cognero.

TIVES: successful cyberattack.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Understand
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 10:08 AM

Multiple Choice

24. Someone who violates computer or Internet security maliciously or for illegal personal gain is known as a(n) _____.
    a. lone wolf attacker
    b. industrial spy
    c. hacktivist
    d. cyberterrorist

ANSWER: a
RATIONALE: A lone wolf attacker is someone who violates computer or Internet security maliciously or for illegal personal gain. Currently, although the lone wolf and cyberterrorist receive a lot of publicity, they are not considered among the most serious sources of cyberattacks.
FEEDBACK:
a. A lone wolf attacker is someone who violates computer or Internet security maliciously or for illegal personal gain.
b. A lone wolf attacker is someone who violates computer or Internet security maliciously or for illegal personal gain.
c. A lone wolf attacker is someone who violates computer or Internet security maliciously or for illegal personal gain.
d. A lone wolf attacker is someone who violates computer or Internet security maliciously or for illegal personal gain.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Perpetrators Most Likely to Initiate a Cyberattack
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.2 - Identify four classes of perpetrators mostly likely to initiate a cyberattack.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 10:13 AM

25. A hacktivist is someone who _____.
    a. attempts to gain financially and/or disrupt a company's information systems and business operations
    b. hacks computers or Web sites in an attempt to promote a political ideology
    c. attempts to destroy the infrastructure components of governments
    d. violates computer or Internet security maliciously or for illegal personal gain

ANSWER: b
RATIONALE: A hacktivist is an individual who hacks computers or Web sites in order to promote a political

Copyright Cengage Learning. Powered by Cognero.

ideology.

FEEDBACK:

a. A hacktivist is an individual who hacks computers or Web sites in order to promote a political ideology.
b. A hacktivist is an individual who hacks computers or Web sites in order to promote a political ideology.
c. A hacktivist is an individual who hacks computers or Web sites in order to promote a political ideology.
d. A hacktivist is an individual who hacks computers or Web sites in order to promote a political ideology.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Perpetrators Most Likely to Initiate a Cyberattack
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.2 - Identify four classes of perpetrators mostly likely to initiate a cyberattack.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 11:07 AM

26. These days, the biggest threats to IT security are from _____.

a. “geeks” working on their own and motivated by the desire to gain some degree of notoriety
b. international drug cartels
c. terrorist organizations
d. organized groups that have ample resources, including money and sophisticated tools, to support their efforts

ANSWER: d

RATIONALE: Previously, computer troublemakers were stereotyped as introverted “geeks” who were working independently and who were motivated by the desire to gain some degree of notoriety. These individuals were armed with specialized, but limited, knowledge of computers and networks and used rudimentary tools, perhaps downloaded from the Internet, to execute exploits. While such individuals still exist, today’s computer menace is much better organized and may be part of an organized group (such as Anonymous, Chaos Computer Club, Lizard Squad, TeslaTeam) that has an agenda and that targets specific organizations and Web sites. Some of these groups have ample resources, including money and sophisticated tools, to support their efforts.

FEEDBACK:

a. Today’s computer menace is much better organized and may be part of an organized group that has an agenda and that targets specific organizations and Web sites. Some of these groups have ample resources, including money and sophisticated tools, to support their efforts.
b. Today’s computer menace is much better organized and may be part of an organized group that has an agenda and that targets specific organizations and Web sites. Some of these groups have ample resources, including money and sophisticated tools, to support their efforts.
c. Today’s computer menace is much better organized and may be part of an organized group that has an agenda and that targets specific organizations and Web sites. Some of these groups have ample resources, including money and sophisticated tools, to support their efforts.
d. Today’s computer menace is much better organized and may be part of an organized

group that has an agenda and that targets specific organizations and Web sites. Some of these groups have ample resources, including money and sophisticated tools, to support their efforts.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Why Computer Incidents Are So Prevalent
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.1 - State four reasons why computer incidents have become so prevalent.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 11:13 AM

27. Your business has a web server that has suddenly become unresponsive. When you study the server's logs there are a huge number of requests from what appear to be legitimate computers. The problem is likely because of _____.

a. a CAPTCHA issue
b. a distributed denial-of-service attack
c. too many Spam emails
d. a logic bomb

ANSWER: b
RATIONALE: A distributed denial-of-service (DDoS) attack is one in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks. The target computers become so overwhelmed by requests for service that legitimate users are unable to get through to the target computer.
FEEDBACK:
a. A distributed denial-of-service (DDoS) attack is one in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks.
b. A distributed denial-of-service (DDoS) attack is one in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks.
c. A distributed denial-of-service (DDoS) attack is one in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks.
d. A distributed denial-of-service (DDoS) attack is one in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks.

POINTS: 1
DIFFICULTY: Moderate
REFERENCES: Cyberattacks That Pose Serious Threats
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.5 - Identify five cyberthreats that pose a serious threat for organizations.
NATIONAL STANDARDS: United States - BUSPROG: Technology

Copyright Cengage Learning. Powered by Cognero.

ARDS:
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 11:19 AM

28. A botnet is a ____.
    a. network of robots that control an assembly line at a factory
    b. network of servers that exchange traffic data
    c. network of devices that are used for managing security
    d. network of computers that send out access requests to servers repeatedly

ANSWER: d
RATIONALE: The term botnet is used to describe a large group of such computers, which are controlled from one or more remote locations by hackers, without the knowledge or consent of their legitimate owners. Based on a command by the attacker or at a preset time, the botnet computers (called zombies) go into action, each sending a simple request for access to the target site again and again—dozens of times per second.
FEEDBACK:
a. The term botnet is used to describe a large group of such computers, which are controlled from one or more remote locations by hackers, without the knowledge or consent of their legitimate owners. Based on a command by the attacker or at a preset time, the botnet computers (called zombies) go into action, each sending a simple request for access to the target site again and again—dozens of times per second.
b. The term botnet is used to describe a large group of such computers, which are controlled from one or more remote locations by hackers, without the knowledge or consent of their legitimate owners. Based on a command by the attacker or at a preset time, the botnet computers (called zombies) go into action, each sending a simple request for access to the target site again and again—dozens of times per second.
c. The term botnet is used to describe a large group of such computers, which are controlled from one or more remote locations by hackers, without the knowledge or consent of their legitimate owners. Based on a command by the attacker or at a preset time, the botnet computers (called zombies) go into action, each sending a simple request for access to the target site again and again—dozens of times per second.
d. The term botnet is used to describe a large group of such computers, which are controlled from one or more remote locations by hackers, without the knowledge or consent of their legitimate owners. Based on a command by the attacker or at a preset time, the botnet computers (called zombies) go into action, each sending a simple request for access to the target site again and again—dozens of times per second.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Cyberattacks That Pose Serious Threats
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.5 - Identify five cyberthreats that pose a serious threat for organizations.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 11:22 AM

Copyright Cengage Learning. Powered by Cognero.

29. Once a _____ is installed, the attacker can gain full access to the computer.

a. botnet
b. zombie
c. worm
d. rootkit

ANSWER: d

RATIONALE: There are numerous types of attack vectors. One is a rootkit, a set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge. Once installed, the attacker can gain full control of the system and even obscure the presence of the rootkit from legitimate system administrators.

FEEDBACK:

a. Once a rootkit is installed, the attacker can gain full control of the system and even obscure the presence of the rootkit from legitimate system administrators.
b. Once a rootkit is installed, the attacker can gain full control of the system and even obscure the presence of the rootkit from legitimate system administrators.
c. Once a rootkit is installed, the attacker can gain full control of the system and even obscure the presence of the rootkit from legitimate system administrators.
d. Once a rootkit is installed, the attacker can gain full control of the system and even obscure the presence of the rootkit from legitimate system administrators.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Types of Attack Vectors
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.4 - Identify at least three commonly used attack vectors.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 11:27 AM

30. The purpose of an advanced persistent threat usually is to ____.

a. steal money
b. interrupt service
c. steal data
d. annoy the users

ANSWER: c

RATIONALE: There are numerous types of attack vectors. One is an advanced persistent threat, a network attack in which an intruder gains access to a network and stays there—undetected—with the intention of stealing data over a long period of time.

FEEDBACK:

a. An advanced persistent threat is a network attack in which an intruder gains access to a network and stays there—undetected—with the intention of stealing data over a long period of time.
b. An advanced persistent threat is a network attack in which an intruder gains access to a network and stays there—undetected—with the intention of stealing data over a long period of time.
c. An advanced persistent threat is a network attack in which an intruder gains access to

Copyright Cengage Learning. Powered by Cognero.

a network and stays there—undetected—with the intention of stealing data over a long period of time.

d. An advanced persistent threat is a network attack in which an intruder gains access to a network and stays there—undetected—with the intention of stealing data over a long period of time.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Types of Attack Vectors
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.4 - Identify at least three commonly used attack vectors.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 11:31 AM

31. The US-CERT incident reporting system is used to ____.

a. alert the bank about stolen credit cards
b. alert the government about missing computers
c. alert the Border Patrol about undocumented workers
d. alert the Department of Homeland Security about information security incidents

ANSWER: d
RATIONALE: The Department of Homeland Security Web site (www.dhs.gov) provides a link that enables users to report cyber incidents. Incident reports go to the US-CERT Incident Reporting System, which assists analysts of the U.S. Computer Emergency Readiness Team (US-CERT) (a partnership between the Department of Homeland Security and the public and private sectors) in providing timely handling of security incidents as well as in conducting improved analysis of such incidents. Established in 2003 to protect the nation's Internet infrastructure against cyberattacks, US-CERT serves as a clearinghouse for information on new viruses, worms, and other computer security topics.
FEEDBACK:

a. Incident reports go to the US-CERT Incident Reporting System, which assists analysts of the U.S. Computer Emergency Readiness Team (US-CERT) (a partnership between the Department of Homeland Security and the public and private sectors) in providing timely handling of security incidents as well as in conducting improved analysis of such incidents.

b. Incident reports go to the US-CERT Incident Reporting System, which assists analysts of the U.S. Computer Emergency Readiness Team (US-CERT) (a partnership between the Department of Homeland Security and the public and private sectors) in providing timely handling of security incidents as well as in conducting improved analysis of such incidents.

c. Incident reports go to the US-CERT Incident Reporting System, which assists analysts of the U.S. Computer Emergency Readiness Team (US-CERT) (a partnership between the Department of Homeland Security and the public and private sectors) in providing timely handling of security incidents as well as in conducting improved analysis of such incidents.

d. Incident reports go to the US-CERT Incident Reporting System, which assists analysts of the U.S. Computer Emergency Readiness Team (US-CERT) (a partnership between the Department of Homeland Security and the public and private sectors) in providing

Copyright Cengage Learning. Powered by Cognero.

timely handling of security incidents as well as in conducting improved analysis of such incidents.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Cyberattacks That Pose Serious Threats
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.5 - Identify five cyberthreats that pose a serious threat for organizations.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 4:07 PM

32. In a denial-of-service (DDoS) attack, the perpetrator ____.
    a. instructs the zombie computers to send simple access requests to target computers
    b. sends out a huge number of spam emails to everyone in your contacts list
    c. changes the configuration information of the infected computers
    d. refuses to accept any email from any sender

ANSWER: a
RATIONALE: In a DDoS attack, a tiny program is downloaded surreptitiously from the attacker's computer to dozens, hundreds, or even thousands of computers all over the world. The term botnet is used to describe a large group of such computers, which are controlled from one or more remote locations by hackers, without the knowledge or consent of their legitimate owners. Based on a command by the attacker or at a preset time, the botnet computers (called zombies) go into action, each sending a simple request for access to the target site again and again—dozens of times per second.
FEEDBACK:
    a. In a DDoS attack, based on a command by the attacker or at a preset time, the botnet computers (called zombies) each send a simple request for access to the target site again and again—dozens of times per second.
    b. In a DDoS attack, based on a command by the attacker or at a preset time, the botnet computers (called zombies) each send a simple request for access to the target site again and again—dozens of times per second.
    c. In a DDoS attack, based on a command by the attacker or at a preset time, the botnet computers (called zombies) each send a simple request for access to the target site again and again—dozens of times per second.
    d. In a DDoS attack, based on a command by the attacker or at a preset time, the botnet computers (called zombies) each send a simple request for access to the target site again and again—dozens of times per second.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Cyberattacks That Pose Serious Threats
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.5 - Identify five cyberthreats that pose a serious threat for organizations.
NATIONAL STANDARDS: United States - BUSPROG: Technology

Copyright Cengage Learning. Powered by Cognero.

ARDS:
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 4:14 PM

33. A company's risk assessment process can consider numerous threats to the computers and networks. Which of the following should an organization identify as loss events or threats to assess?

a. distributed denial-of-service attack
b. email attachment with harmful worm
c. harmful virus
d. all of the above

ANSWER: d
RATIONALE: Step 2 of the risk assessment process is to identify the loss events or the risks or threats that could occur. Table 2.4 identifies the following examples of such adverse events: data breach of customer account data, distributed denial-of-service (DDoS) attack, email attachment with harmful worm, harmful viruses, and invoice and payment fraud.
FEEDBACK:
a. Table 2.4 identifies the following examples of such adverse events: data breach of customer account data, distributed denial-of-service (DDoS) attack, email attachment with harmful worm, harmful viruses, and invoice and payment fraud.
b. Table 2.4 identifies the following examples of such adverse events: data breach of customer account data, distributed denial-of-service (DDoS) attack, email attachment with harmful worm, harmful viruses, and invoice and payment fraud.
c. Table 2.4 identifies the following examples of such adverse events: data breach of customer account data, distributed denial-of-service (DDoS) attack, email attachment with harmful worm, harmful viruses, and invoice and payment fraud.
d. Table 2.4 identifies the following examples of such adverse events: data breach of customer account data, distributed denial-of-service (DDoS) attack, email attachment with harmful worm, harmful viruses, and invoice and payment fraud.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the Organizational Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization, network, application, and end user levels to safeguard against cyberattacks.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 4:25 PM

34. Which of the following laws covers false claims regarding unauthorized use of credit cards?

a. Computer Fraud and Abuse Act
b. Fraud and Related Activity in Connection with Access Devices Statute
c. Identity Theft and Assumption Deterrence Act
d. Stored Wire and Electronic Communications and Transactional Records Access Statutes

ANSWER: b

Copyright Cengage Learning. Powered by Cognero.

RATIONALE: The Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029) covers false claims regarding unauthorized use of credit cards.

FEEDBACK:

a. The Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029) covers false claims regarding unauthorized use of credit cards.
b. The Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029) covers false claims regarding unauthorized use of credit cards.
c. The Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029) covers false claims regarding unauthorized use of credit cards.
d. The Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029) covers false claims regarding unauthorized use of credit cards.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Federal Laws for Prosecuting Computer Attacks
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.7 - Identify five federal laws that address computer crime.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 4:29 PM

35. Which of the following activities does the USA Patriot Act define?

a. cyberterrorism
b. identity theft
c. credit card fraud
d. transmitting virus programs

ANSWER: a
RATIONALE: The USA Patriot Act defines cyberterrorism and associated penalties.
FEEDBACK:

a. The USA Patriot Act defines cyberterrorism and associated penalties.
b. The USA Patriot Act defines cyberterrorism and associated penalties.
c. The USA Patriot Act defines cyberterrorism and associated penalties.
d. The USA Patriot Act defines cyberterrorism and associated penalties.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Federal Laws for Prosecuting Computer Attacks
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.7 - Identify five federal laws that address computer crime.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 4:31 PM

Copyright Cengage Learning. Powered by Cognero.

36. Which of these organizations offers guidelines on developing security policies?

a. DHS
b. SANS
c. IBM
d. CISCO

ANSWER: b

RATIONALE: The SANS (SysAdmin, Audit, Network, Security) Institute's Web site (www.sans.org) offers several security-related policy templates that can help an organization to quickly develop effective security policies.

FEEDBACK:

a. The SANS (SysAdmin, Audit, Network, Security) Institute's Web site offers several security-related policy templates that can help an organization to quickly develop effective security policies.
b. The SANS (SysAdmin, Audit, Network, Security) Institute's Web site offers several security-related policy templates that can help an organization to quickly develop effective security policies.
c. The SANS (SysAdmin, Audit, Network, Security) Institute's Web site offers several security-related policy templates that can help an organization to quickly develop effective security policies.
d. The SANS (SysAdmin, Audit, Network, Security) Institute's Web site offers several security-related policy templates that can help an organization to quickly develop effective security policies.

POINTS: 1

DIFFICULTY: Easy

REFERENCES: Implementing CIA at the Organizational Level

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization, network, application, and end user levels to safeguard against cyberattacks.

NATIONAL STANDARDS: United States - BUSPROG: Technology

KEYWORDS: Bloom's: Remember

DATE CREATED: 11/19/2019 5:58 PM

DATE MODIFIED: 12/26/2019 4:34 PM

37. You have been hired as the new Information Security consultant at XYZ Inc. Which of these employee behaviors would be a top security concern?

a. leaving laptop computers unattended in public spaces
b. using office computers for personal emails
c. drinking water or coffee while working on computers
d. banging on the keyboard when the computer is running slowly

ANSWER: a

RATIONALE: Employees and contract workers must be educated about the importance of security so that they will be motivated to understand and follow security policies. Users must understand that they are a key part of the security system and that they have certain responsibilities. For example, users must help protect an organization's information systems and data by taking care to ensure that portable computing and data storage devices are protected (hundreds of thousands of laptops are lost or stolen per year).

Copyright Cengage Learning. Powered by Cognero.

FEEDBACK:

a. Users must understand that they are a key part of the security system and that they have certain responsibilities. For example, users must help protect an organization's information systems and data by taking care to ensure that portable computing and data storage devices are protected.

b. Users must understand that they are a key part of the security system and that they have certain responsibilities. For example, users must help protect an organization's information systems and data by taking care to ensure that portable computing and data storage devices are protected.

c. Users must understand that they are a key part of the security system and that they have certain responsibilities. For example, users must help protect an organization's information systems and data by taking care to ensure that portable computing and data storage devices are protected.

d. Users must understand that they are a key part of the security system and that they have certain responsibilities. For example, users must help protect an organization's information systems and data by taking care to ensure that portable computing and data storage devices are protected.

POINTS: 1

DIFFICULTY: Moderate

REFERENCES: Implementing CIA at the End-User Level

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization, network, application, and end user levels to safeguard against cyberattacks.

NATIONAL STANDARDS: United States - BUSPROG: Technology

KEYWORDS: Bloom's: Understand

DATE CREATED: 11/19/2019 5:58 PM

DATE MODIFIED: 12/26/2019 4:38 PM

38. Which of the following is the correct description of a firewall?

a. software that deletes viruses from attachments

b. hardware that prevents unauthorized data from entering a private network

c. a software and hardware combination that limits incoming and outgoing Internet traffic

d. a concept used in developing security policies

ANSWER: c

RATIONALE: A firewall is a system of software, hardware, or a combination of both that stands guard between an organization's internal network and the Internet, and limits network access based on the organization's access policy. Any Internet traffic that is not explicitly permitted into the internal network is denied entry through a firewall. Similarly, most firewalls can be configured so that internal network users can be blocked from gaining access to Web sites deemed inappropriate for employees.

FEEDBACK:

a. A firewall is a system of software, hardware, or a combination of both that stands guard between an organization's internal network and the Internet, and limits network access based on the organization's access policy.

b. A firewall is a system of software, hardware, or a combination of both that stands guard between an organization's internal network and the Internet, and limits network access based on the organization's access policy.

c. A firewall is a system of software, hardware, or a combination of both that stands guard between an organization's internal network and the Internet, and limits network access based on the organization's access policy.

Copyright Cengage Learning. Powered by Cognero.

d. A firewall is a system of software, hardware, or a combination of both that stands guard between an organization's internal network and the Internet, and limits network access based on the organization's access policy.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the Network Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization, network, application, and end user levels to safeguard against cyberattacks.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Understand
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 4:42 PM

39. Which of the following is **NOT** a popular vendor of firewall software?

a. Red Hat
b. Check Point
c. Kaspersky
d. Total Defense

ANSWER: a
RATIONALE: Software vendors Agnitum, Check Point, Comodo, Kaspersky, and Total Defense provide some of the top-rated firewall software used to protect personal computers. Their software provides antivirus, firewall, antispam, parental control, and phishing protection capabilities and sell for $30–$80 per single user license.
FEEDBACK:

a. Software vendors Agnitum, Check Point, Comodo, Kaspersky, and Total Defense provide some of the top-rated firewall software used to protect personal computers.
b. Software vendors Agnitum, Check Point, Comodo, Kaspersky, and Total Defense provide some of the top-rated firewall software used to protect personal computers.
c. Software vendors Agnitum, Check Point, Comodo, Kaspersky, and Total Defense provide some of the top-rated firewall software used to protect personal computers.
d. Software vendors Agnitum, Check Point, Comodo, Kaspersky, and Total Defense provide some of the top-rated firewall software used to protect personal computers.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the Network Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization, network, application, and end user levels to safeguard against cyberattacks.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 4:44 PM

Copyright Cengage Learning. Powered by Cognero.

40. You work for a company that is growing. Originally, all the users in all departments had access to all the data in the database. It is considered a security risk. What is an appropriate action to reduce the risk?

a. Install a two-step login procedure, where the user has to key in additional information for logging in.
b. Install and provide stronger anti-virus software on the users' computers.
c. Tweak the firewall parameters so that outgoing traffic can be better controlled.
d. Assign roles and privileges to users so that only job-relevant data is accessible to the user.

ANSWER: d

RATIONALE: An important safeguard at the application level is the creation of roles and user accounts so that once users are authenticated, they have the authority to perform their responsibilities and nothing more. Even within one department, not all members should be given the same capabilities.

FEEDBACK:

a. An important safeguard at the application level is the creation of roles and user accounts so that once users are authenticated, they have the authority to perform their responsibilities and nothing more.
b. An important safeguard at the application level is the creation of roles and user accounts so that once users are authenticated, they have the authority to perform their responsibilities and nothing more.
c. An important safeguard at the application level is the creation of roles and user accounts so that once users are authenticated, they have the authority to perform their responsibilities and nothing more.
d. An important safeguard at the application level is the creation of roles and user accounts so that once users are authenticated, they have the authority to perform their responsibilities and nothing more.

POINTS: 1
DIFFICULTY: Moderate
REFERENCES: Implementing CIA at the Application Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization, network, application, and end user levels to safeguard against cyberattacks.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Understand
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 4:48 PM

41. Which of the following shortcomings may be revealed during an IT security audit?

a. whether the IT budget is adequate or not
b. whether the users are satisfied with IT services or not
c. whether only the appropriate personnel have access to critical data
d. whether the firewall is tall enough

ANSWER: c

RATIONALE: The security audit should review who has access to key systems and data and what level of authority each user has. It is not unusual for an audit to reveal that too many people have access to critical data and that many people have capabilities beyond those needed to perform their jobs.

FEEDBACK:

a. The security audit should review who has access to key systems and data and what level of authority each user has. It is not unusual for an audit to reveal that too many people have access to critical data and that many people have capabilities beyond those needed to perform their jobs.

Copyright Cengage Learning. Powered by Cognero.

b. The security audit should review who has access to key systems and data and what level of authority each user has. It is not unusual for an audit to reveal that too many people have access to critical data and that many people have capabilities beyond those needed to perform their jobs.

c. The security audit should review who has access to key systems and data and what level of authority each user has. It is not unusual for an audit to reveal that too many people have access to critical data and that many people have capabilities beyond those needed to perform their jobs.

d. The security audit should review who has access to key systems and data and what level of authority each user has. It is not unusual for an audit to reveal that too many people have access to critical data and that many people have capabilities beyond those needed to perform their jobs.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the Organizational Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization, network, application, and end user levels to safeguard against cyberattacks.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 4:54 PM

42. Assume your organization is experiencing an intruder attack. You have an intrusion detection system (IDS) set up. Which of the following events occurs first?

a. Messages from the IDS are routed to the network security team.
b. The IDS warns the firewall of suspicious traffic.
c. The network router sends traffic to the firewall as well as to the IDS.
d. The network security team decides to block traffic from that IP address.

ANSWER: c
RATIONALE: An intrusion detection system (IDS) is software and/or hardware that monitors system and network resources and activities and notifies network security personnel when it detects network traffic that attempts to circumvent the security measures of a networked computer environment. Figure 2.8 shows that the first step in the process is that the organization's network router sends network traffic to both IDS and firewall.
FEEDBACK:

a. Figure 2.8 shows that the first step in the process is that the organization's network router sends network traffic to both IDS and firewall.

b. Figure 2.8 shows that the first step in the process is that the organization's network router sends network traffic to both IDS and firewall.

c. Figure 2.8 shows that the first step in the process is that the organization's network router sends network traffic to both IDS and firewall.

d. Figure 2.8 shows that the first step in the process is that the organization's network router sends network traffic to both IDS and firewall.

POINTS: 1
DIFFICULTY: Moderate
REFERENCES: Detection of a Cyberattack

Copyright Cengage Learning. Powered by Cognero.

QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization, network, application, and end user levels to safeguard against cyberattacks.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Understand
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/26/2019 4:58 PM

43. Which of the following security incidents is least costly to fix?

a. theft of program source code
b. alteration of corporate database
c. theft of trade secrets
d. defacing of web pages

ANSWER: d
RATIONALE: If a Web site was simply defaced, it is easy to fix or restore the site's HTML (Hypertext Markup Language—the code that describes to your browser how a Web page should look). However, what if the intruders inflicted more serious damage, such as erasing proprietary program source code or the contents of key corporate databases? What if they stole company trade secrets? Expert crackers can conceal their identity and tracking them down can take a long time as well as a tremendous amount of corporate resources.
FEEDBACK:
a. If a Web site was simply defaced, it is easy to fix or restore the site's HTML.
b. If a Web site was simply defaced, it is easy to fix or restore the site's HTML.
c. If a Web site was simply defaced, it is easy to fix or restore the site's HTML.
d. If a Web site was simply defaced, it is easy to fix or restore the site's HTML.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Response
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.11 - Describe five actions an organization must take in response to a successful cyberattack.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Understand
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/27/2019 12:06 PM

44. A data breach at your business resulted in the loss of some customer data. Several angry customers have filed charges. What is a recommended course of action to prepare for future events?

a. activate the forensics analysis team and prepare documentation
b. meet with your lawyers to prepare to counter-sue the customers
c. settle with the customers, however much it may cost
d. none of these answers

ANSWER: a

Copyright Cengage Learning. Powered by Cognero.

RATIONALE: Computer forensics is a discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law. A computer forensics investigation may be opened in response to a criminal investigation or civil litigation. It may also be launched for a variety of other reasons, for example, to retrace steps taken when data has been lost, assess damage following a computer incident, investigate the unauthorized disclosure of personal or corporate confidential data, or to confirm or evaluate the impact of industrial espionage.

FEEDBACK:

a. A computer forensics investigation may be opened in response to a criminal investigation or civil litigation, to retrace steps taken when data has been lost, or to assess damage following a computer incident.

b. A computer forensics investigation may be opened in response to a criminal investigation or civil litigation, to retrace steps taken when data has been lost, or to assess damage following a computer incident.

c. A computer forensics investigation may be opened in response to a criminal investigation or civil litigation, to retrace steps taken when data has been lost, or to assess damage following a computer incident.

d. A computer forensics investigation may be opened in response to a criminal investigation or civil litigation, to retrace steps taken when data has been lost, or to assess damage following a computer incident.

POINTS: 1

DIFFICULTY: Moderate

REFERENCES: Computer Forensics

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

LEARNING OBJECTIVES: POIS.14e.2.13 - Define the term computer forensics.

NATIONAL STANDARDS: United States - BUSPROG: Technology

KEYWORDS: Bloom's: Remember

DATE CREATED: 11/19/2019 5:58 PM

DATE MODIFIED: 12/27/2019 12:14 PM

45. You wish to use your personal laptop computer at work, but the IT department folks will not allow this. The likely reason is that _____.

a. you will use your laptop for non-work-related activities
b. your productivity could not be accurately measured
c. your non-work-related use of the laptop could increase vulnerability
d. your activities could not be monitored

ANSWER: c

RATIONALE: Bring your own device (BYOD) is a business policy that permits, and in some cases encourages, employees to use their own mobile devices (smartphones, tablets, or laptops) to access company computing resources and applications. This practice raises many potential security issues as it is highly likely that such devices are also used for nonwork activity, such as browsing Web sites, blogging, shopping, and visiting social networks. This nonwork activity exposes the devices to malware much more frequently than a device that is used strictly for business purposes.

FEEDBACK:

a. It is highly likely that personal devices are also used for nonwork activity, which exposes the devices to malware much more frequently than a device that is used strictly for business purposes.

Copyright Cengage Learning. Powered by Cognero.

b. It is highly likely that personal devices are also used for nonwork activity, which exposes the devices to malware much more frequently than a device that is used strictly for business purposes.
c. It is highly likely that personal devices are also used for nonwork activity, which exposes the devices to malware much more frequently than a device that is used strictly for business purposes.
d. It is highly likely that personal devices are also used for nonwork activity, which exposes the devices to malware much more frequently than a device that is used strictly for business purposes.

POINTS: 1
DIFFICULTY: Moderate
REFERENCES: Why Computer Incidents Are So Prevalent
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.1 - State four reasons why computer incidents have become so prevalent.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/27/2019 12:23 PM

46. Which of the following companies develops one of the most widely used antivirus software products?

a. Microsoft
b. Symantec
c. US-CERT
d. Agnitum

ANSWER: b
RATIONALE: Good antivirus software checks vital system files when the system is booted up, monitors the system continuously for virus-like activity, scans disks, scans memory when a program is run, checks programs when they are downloaded, and scans email attachments before they are opened. Two of the most widely used antivirus software products are Norton AntiVirus from Symantec and Personal Firewall from McAfee.
FEEDBACK:
a. Two of the most widely used antivirus software products are Norton AntiVirus from Symantec and Personal Firewall from McAfee.
b. Two of the most widely used antivirus software products are Norton AntiVirus from Symantec and Personal Firewall from McAfee.
c. Two of the most widely used antivirus software products are Norton AntiVirus from Symantec and Personal Firewall from McAfee.
d. Two of the most widely used antivirus software products are Norton AntiVirus from Symantec and Personal Firewall from McAfee.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the End-User Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization,

TIVES: network, application, and end user levels to safeguard against cyberattacks.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/27/2019 12:30 PM

47. In computing, an attack on an information system that takes advantage of a particular system vulnerability is called a(n) _____.

a. vector
b. exploit
c. DDoS attack
d. data breach

ANSWER: b
RATIONALE: In computing, an exploit is an attack on an information system that takes advantage of a particular system vulnerability. Often this attack is made possible due to poor system design or implementation.
FEEDBACK:
a. In computing, an exploit is an attack on an information system that takes advantage of a particular system vulnerability.
b. In computing, an exploit is an attack on an information system that takes advantage of a particular system vulnerability.
c. In computing, an exploit is an attack on an information system that takes advantage of a particular system vulnerability.
d. In computing, an exploit is an attack on an information system that takes advantage of a particular system vulnerability.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Why Computer Incidents Are So Prevalent
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.1 - State four reasons why computer incidents have become so prevalent.
KEYWORDS: Blooms's: Remember
DATE CREATED: 12/27/2019 12:38 PM
DATE MODIFIED: 12/27/2019 12:42 PM

48. Someone who attempts to destroy the infrastructure components of governments is known as a _____.

a. cybercriminal
b. lone wolf attacker
c. cyberterrorist
d. hacktivist

ANSWER: c
RATIONALE: A cyberterrorist is a state-sponsored individual or group who attempts to destroy the infrastructure components of governments, financial institutions, corporations, utilities, and emergency response units. Currently, although the lone wolf and cyberterrorist receive a lot of publicity, they are not considered among the most serious sources of cyberattacks.

Copyright Cengage Learning. Powered by Cognero.

FEEDBACK:

a. A cyberterrorist is a state-sponsored individual or group who attempts to destroy the infrastructure components of governments, financial institutions, corporations, utilities, and emergency response units.
b. A cyberterrorist is a state-sponsored individual or group who attempts to destroy the infrastructure components of governments, financial institutions, corporations, utilities, and emergency response units.
c. A cyberterrorist is a state-sponsored individual or group who attempts to destroy the infrastructure components of governments, financial institutions, corporations, utilities, and emergency response units.
d. A cyberterrorist is a state-sponsored individual or group who attempts to destroy the infrastructure components of governments, financial institutions, corporations, utilities, and emergency response units.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Perpetrators Most Likely to Initiate a Cyberattack
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.2 - Identify four classes of perpetrators mostly likely to initiate a cyberattack.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/27/2019 1:00 PM
DATE MODIFIED: 12/27/2019 1:03 PM

49. The attack vector that relies on email messaging to deceive the victim into revealing personal data is known as _____.

a. phishing
b. a worm
c. a rootkit
d. smishing

ANSWER: a
RATIONALE: There are numerous types of attack vectors. One is phishing, the act of fraudulently using email to try to get the recipient to reveal personal data.

FEEDBACK:

a. There are numerous types of attack vectors. One is phishing, the act of fraudulently using email to try to get the recipient to reveal personal data.
b. There are numerous types of attack vectors. One is phishing, the act of fraudulently using email to try to get the recipient to reveal personal data.
c. There are numerous types of attack vectors. One is phishing, the act of fraudulently using email to try to get the recipient to reveal personal data.
d. There are numerous types of attack vectors. One is phishing, the act of fraudulently using email to try to get the recipient to reveal personal data.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Types of Attack Vectors
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.3 - Define the term attack vector.
KEYWORDS: Bloom's: Remember

Copyright Cengage Learning. Powered by Cognero.

DATE CREATED: 12/27/2019 1:08 PM
DATE MODIFIED: 12/27/2019 1:12 PM

50. A hacker writes some programming code that will cause a computer to behave in an unexpected and undesirable manner, but disguises it as something else to make it difficult to detect. Which attack vector has this attacker chosen to use?

a. rootkit
b. worm
c. vishing
d. virus

ANSWER: d
RATIONALE: There are numerous types of attack vectors. One is a virus, a piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner.
FEEDBACK:
a. There are numerous types of attack vectors. One is a virus, a piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner.
b. There are numerous types of attack vectors. One is a virus, a piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner.
c. There are numerous types of attack vectors. One is a virus, a piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner.
d. There are numerous types of attack vectors. One is a virus, a piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Types of Attack Vectors
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.3 - Define the term attack vector.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/27/2019 1:26 PM
DATE MODIFIED: 12/27/2019 1:31 PM

51. Brandon, a security specialist, explains that IS security managers must use their judgment to ensure that the cost of security risk control does not exceed the system's benefits or the risks involved. Brandon is discussing the concept of _____.

a. reasonable assurance
b. business continuity
c. disaster recovery
d. the CIA security triad

ANSWER: a
RATIONALE: Step 7 of risk assessment is to perform a cost-benefit analysis to ensure that your efforts will be cost effective. No amount of resources can guarantee a perfect security system, so organizations must balance the risk of a security breach with the cost of preventing one. The concept of reasonable

Copyright Cengage Learning. Powered by Cognero.

assurance in connection with IT security recognizes that managers must use their judgment to ensure that the cost of control does not exceed the system's benefits or the risks involved.

FEEDBACK:

a. The concept of reasonable assurance in connection with IT security recognizes that managers must use their judgment to ensure that the cost of control does not exceed the system's benefits or the risks involved.

b. The concept of reasonable assurance in connection with IT security recognizes that managers must use their judgment to ensure that the cost of control does not exceed the system's benefits or the risks involved.

c. The concept of reasonable assurance in connection with IT security recognizes that managers must use their judgment to ensure that the cost of control does not exceed the system's benefits or the risks involved.

d. The concept of reasonable assurance in connection with IT security recognizes that managers must use their judgment to ensure that the cost of control does not exceed the system's benefits or the risks involved.

POINTS: 1

DIFFICULTY: Easy

REFERENCES: Implementing CIA at the Organizational Level

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

LEARNING OBJECTIVES: POIS.14e.2.10 - Identify eight steps that must be taken to perform a thorough security risk assessment.

KEYWORDS: Bloom's: Remember

DATE CREATED: 12/27/2019 1:40 PM

DATE MODIFIED: 12/27/2019 1:45 PM

52. Your ex-colleague was apprehended and charged with a crime based on the Fraud and Related Activity in Connection with Access Devices Statute. He was caught using unauthorized or stolen _____.

a. computer passwords

b. email addresses

c. application code

d. credit cards

ANSWER: d

RATIONALE: Over the years, the United States Congress has enacted multiple laws to help prosecute those responsible for computer-related crime. The Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029) covers false claims regarding unauthorized use of credit cards.

FEEDBACK:

a. The Fraud and Related Activity in Connection with Access Devices Statute covers false claims regarding unauthorized use of credit cards.

b. The Fraud and Related Activity in Connection with Access Devices Statute covers false claims regarding unauthorized use of credit cards.

c. The Fraud and Related Activity in Connection with Access Devices Statute covers false claims regarding unauthorized use of credit cards.

d. The Fraud and Related Activity in Connection with Access Devices Statute covers false claims regarding unauthorized use of credit cards.

POINTS: 1

DIFFICULTY: Easy

REFERENCES: Federal Laws for Prosecuting Computer Attacks

QUESTION TYPE: Multiple Choice

Copyright Cengage Learning. Powered by Cognero.

HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.7 - Identify five federal laws that address computer crime.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/27/2019 1:50 PM
DATE MODIFIED: 12/27/2019 1:53 PM

53. The US-CERT newsletter has alerted you about a specific vulnerability in some software installed on your organization's computers. To detect any attempts at exploiting this vulnerability, you employ a(n) ____-based intrusion detection system.

a. incident
b. knowledge
c. behavior
d. firewall

ANSWER: b
RATIONALE: Knowledge-based approaches and behavior-based approaches are two fundamentally different approaches to intrusion detection. Knowledge-based intrusion detection systems contain information about specific attacks and system vulnerabilities and watch for attempts to exploit these vulnerabilities, such as repeated failed login attempts or recurring attempts to download a program to a server. When such an attempt is detected, an alarm is triggered.
FEEDBACK:
a. Knowledge-based intrusion detection systems contain information about specific attacks and system vulnerabilities and watch for attempts to exploit these vulnerabilities.
b. Knowledge-based intrusion detection systems contain information about specific attacks and system vulnerabilities and watch for attempts to exploit these vulnerabilities.
c. Knowledge-based intrusion detection systems contain information about specific attacks and system vulnerabilities and watch for attempts to exploit these vulnerabilities.
d. Knowledge-based intrusion detection systems contain information about specific attacks and system vulnerabilities and watch for attempts to exploit these vulnerabilities.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Detection of a Cyberattack
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.11 - Describe five actions an organization must take in response to a successful cyberattack.
KEYWORDS: Bloom's: Understand
DATE CREATED: 12/27/2019 1:59 PM
DATE MODIFIED: 12/27/2019 2:04 PM

54. Many organizations outsource their network security operations to a(n) _____.

a. VPN
b. HIPAA
c. MSSP

Copyright Cengage Learning. Powered by Cognero.

d. CSFA

ANSWER: c

RATIONALE: For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations can be too costly to acquire and maintain. As a result, many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.

FEEDBACK:

a. Many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.

b. Many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.

c. Many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.

d. Many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.

POINTS: 1

DIFFICULTY: Easy

REFERENCES: Using a Managed Security Service Provider (MSSP)

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

LEARNING OBJECTIVES: POIS.14e.2.12 - Describe the role of a managed security service provider.

KEYWORDS: Bloom's: Remember

DATE CREATED: 12/27/2019 2:06 PM

DATE MODIFIED: 12/27/2019 2:11 PM

55. What discipline combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law?

a. CIA implementation

b. risk assessment

c. computer forensics

d. security policy

ANSWER: c

RATIONALE: Computer forensics is a discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law.

FEEDBACK:

a. Computer forensics is a discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law.

b. Computer forensics is a discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it

Copyright Cengage Learning. Powered by Cognero.

is admissible as evidence in a court of law.

c. Computer forensics is a discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law.

d. Computer forensics is a discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Computer Forensics
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.13 - Define the term computer forensics.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/27/2019 2:13 PM
DATE MODIFIED: 12/27/2019 2:17 PM

56. Which of the following is considered the most likely source of cyberattacks, based on a poll of global executives, information security managers, and IT leaders?

a. lone wolf attackers
b. careless insiders
c. cyberterrorists
d. MSSPs

ANSWER: b
RATIONALE: In 2017–2018, professional service firm Ernst & Young polled 1,735 global executives, information security managers, and IT leaders, and found that in descending order, careless insiders, cyber criminals, malicious employees, and hacktivists were considered the most likely sources of a cyberattack. Currently, although the lone wolf and cyberterrorist receive a lot of publicity, they are not considered among the most serious sources of cyberattacks.
FEEDBACK:

a. In descending order, careless insiders, cyber criminals, malicious employees, and hacktivists were considered the most likely sources of a cyberattack.

b. In descending order, careless insiders, cyber criminals, malicious employees, and hacktivists were considered the most likely sources of a cyberattack.

c. In descending order, careless insiders, cyber criminals, malicious employees, and hacktivists were considered the most likely sources of a cyberattack.

d. In descending order, careless insiders, cyber criminals, malicious employees, and hacktivists were considered the most likely sources of a cyberattack.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Perpetrators Most Likely to Initiate a Cyberattack
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.2 - Identify four classes of perpetrators mostly likely to initiate a cyberattack.

Copyright Cengage Learning. Powered by Cognero.

KEYWORDS: Bloom's: Remember
DATE CREATED: 12/27/2019 3:50 PM
DATE MODIFIED: 12/27/2019 3:55 PM

57. You discover that one of your organization's computers has stopped working properly due to malware. Who is most likely responsible for the presence of malware on this machine?

a. a "geek" engaged in a prank
b. a malicious individual
c. a state-sponsored hacker
d. a careless coworker

ANSWER: d
RATIONALE: IBM found that 55–60 percent of all cyberattacks are initiated through the actions of insiders. These insiders include employees, business partners, clients, contractors, and consultants who have physical or remote access to a company's assets. Careless (or untrained) insiders might not be acting with criminal intent but they might fail to follow your organization's cybersecurity policies and do something foolish such as creating a weak password or opening an email attachment containing malware.
FEEDBACK:
a. Careless (or untrained) insiders might not be acting with criminal intent but they might fail to follow your organization's cybersecurity policies and do something foolish such as creating a weak password or opening an email attachment containing malware.
b. Careless (or untrained) insiders might not be acting with criminal intent but they might fail to follow your organization's cybersecurity policies and do something foolish such as creating a weak password or opening an email attachment containing malware.
c. Careless (or untrained) insiders might not be acting with criminal intent but they might fail to follow your organization's cybersecurity policies and do something foolish such as creating a weak password or opening an email attachment containing malware.
d. Careless (or untrained) insiders might not be acting with criminal intent but they might fail to follow your organization's cybersecurity policies and do something foolish such as creating a weak password or opening an email attachment containing malware.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Perpetrators Most Likely to Initiate a Cyberattack
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.2 - Identify four classes of perpetrators mostly likely to initiate a cyberattack.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/27/2019 3:56 PM
DATE MODIFIED: 12/27/2019 4:07 PM

58. After being passed over for a promotion, an accountant accesses his firm's database and deletes or alters key information in an effort to take revenge on his superiors. This is an example of a cyberattack initiated by _____.

a. a malicious employee
b. a careless insider
c. a cybercriminal
d. a lone wolf attacker

ANSWER: a

Copyright Cengage Learning. Powered by Cognero.

RATIONALE: IBM found that 55–60 percent of all cyberattacks are initiated through the actions of insiders. These insiders include employees, business partners, clients, contractors, and consultants who have physical or remote access to a company's assets. A malicious employee is an insider who deliberately attempts to gain access to and/or disrupt a company's information systems and business operations.

FEEDBACK:

a. A malicious employee is an insider who deliberately attempts to gain access to and/or disrupt a company's information systems and business operations.
b. A malicious employee is an insider who deliberately attempts to gain access to and/or disrupt a company's information systems and business operations.
c. A malicious employee is an insider who deliberately attempts to gain access to and/or disrupt a company's information systems and business operations.
d. A malicious employee is an insider who deliberately attempts to gain access to and/or disrupt a company's information systems and business operations.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Perpetrators Most Likely to Initiate a Cyberattack
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.2 - Identify four classes of perpetrators mostly likely to initiate a cyberattack.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/27/2019 4:08 PM
DATE MODIFIED: 12/27/2019 4:16 PM

59. Debbie is a programmer who attacks corporate computer networks for financial gain. She is a _____.

a. careless insider
b. malicious insider
c. cyberterrorist
d. cybercriminal

ANSWER: d
RATIONALE: In 2017–2018, professional service firm Ernst & Young polled 1,735 global executives, information security managers, and IT leaders, and found that in descending order, careless insiders, cyber criminals, malicious employees, and hacktivists were considered the most likely sources of a cyberattack. A cybercriminal is someone who attacks a computer system or network for financial gain.

FEEDBACK:

a. A cybercriminal is someone who attacks a computer system or network for financial gain.
b. A cybercriminal is someone who attacks a computer system or network for financial gain.
c. A cybercriminal is someone who attacks a computer system or network for financial gain.
d. A cybercriminal is someone who attacks a computer system or network for financial gain.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Perpetrators Most Likely to Initiate a Cyberattack
QUESTION TYPE: Multiple Choice

Copyright Cengage Learning. Powered by Cognero.

HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.2 - Identify four classes of perpetrators mostly likely to initiate a cyberattack.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/27/2019 4:18 PM
DATE MODIFIED: 12/27/2019 4:22 PM

60. What is an attack vector?

a. a person who attacks a computer system or network for financial gain
b. the technique used to gain unauthorized access to a device or a network
c. a large group of computers controlled from one or more remote locations by hackers
d. a vulnerable communications protocol or system

ANSWER: b
RATIONALE: An attack vector is the technique used to gain unauthorized access to a device or a network.
FEEDBACK:
a. An attack vector is the technique used to gain unauthorized access to a device or a network.
b. An attack vector is the technique used to gain unauthorized access to a device or a network.
c. An attack vector is the technique used to gain unauthorized access to a device or a network.
d. An attack vector is the technique used to gain unauthorized access to a device or a network.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Types of Attack Vectors
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.3 - Define the term attack vector.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/27/2019 4:23 PM
DATE MODIFIED: 12/27/2019 4:29 PM

61. Miles falls prey to a con artist who uses deception to trick him into revealing the data required to access his employer's information system. Miles has experienced an attack vector known as _____.

a. social engineering
b. smishing
c. an advanced persistent threat
d. a Trojan horse

ANSWER: a
RATIONALE: Perpetrators of computer crimes use an attack vector to gain unauthorized access to a device or a network and to initiate a cyberattack. There are numerous types of attack vectors. One is social engineering, the use of deception to trick individuals into divulging data needed to gain access to an information system or network.
FEEDBACK:
a. There are numerous types of attack vectors. One is social engineering, the use of deception to trick individuals into divulging data needed to gain access to an

information system or network.

b. There are numerous types of attack vectors. One is social engineering, the use of deception to trick individuals into divulging data needed to gain access to an information system or network.

c. There are numerous types of attack vectors. One is social engineering, the use of deception to trick individuals into divulging data needed to gain access to an information system or network.

d. There are numerous types of attack vectors. One is social engineering, the use of deception to trick individuals into divulging data needed to gain access to an information system or network.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Types of Attack Vectors
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.3 - Define the term attack vector.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/27/2019 4:30 PM
DATE MODIFIED: 12/27/2019 4:38 PM

62. Viruses and worms are both attack vectors, but they differ in that _____.

a. worms combine the features of a virus, a Trojan horse, and other malicious code
b. viruses are symptomless
c. worms can propagate without human intervention
d. viruses can send copies of themselves to other computers

ANSWER: c
RATIONALE: Perpetrators of computer crimes use an attack vector to gain unauthorized access to a device or a network and to initiate a cyberattack. There are numerous types of attack vectors. One is a virus, a piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner. Another is a worm, a harmful program that resides in the active memory of the computer and duplicates itself. Worms differ from viruses in that they can propagate without human intervention, often sending copies of themselves to other computers by email.
FEEDBACK:

a. Worms differ from viruses in that they can propagate without human intervention, often sending copies of themselves to other computers by email.

b. Worms differ from viruses in that they can propagate without human intervention, often sending copies of themselves to other computers by email.

c. Worms differ from viruses in that they can propagate without human intervention, often sending copies of themselves to other computers by email.

d. Worms differ from viruses in that they can propagate without human intervention, often sending copies of themselves to other computers by email.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Types of Attack Vectors
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False

Copyright Cengage Learning. Powered by Cognero.

LEARNING OBJECTIVES: POIS.14e.2.3 - Define the term attack vector.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/27/2019 4:39 PM
DATE MODIFIED: 12/27/2019 4:45 PM

63. Jennifer is a programmer who develops malware and deploys it in the computer systems of her organization's competitors so that she can secretly steal data about new product plans and designs, thus gaining a competitive advantage for her organization. What type of cyberattack is Jennifer involved in?

a. data breach
b. cyberespionage
c. distributed denial-of-service attack
d. ransomware

ANSWER: b
RATIONALE: Cyberespionage involves the deployment of malware that secretly steals data in the computer systems of organizations. These organizations include government agencies, military contractors, political organizations, and manufacturing firms. The type of data most frequently targeted includes data that can provide an unfair competitive advantage to the perpetrator. This data is typically not public knowledge and may even be protected via patent, copyright, or trade secret.
FEEDBACK:
a. Cyberespionage involves the deployment of malware that secretly steals data in the computer systems of organizations.
b. Cyberespionage involves the deployment of malware that secretly steals data in the computer systems of organizations.
c. Cyberespionage involves the deployment of malware that secretly steals data in the computer systems of organizations.
d. Cyberespionage involves the deployment of malware that secretly steals data in the computer systems of organizations.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Cyberattacks That Pose Serious Threats
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.5 - Identify five cyberthreats that pose a serious threat for organizations.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/27/2019 4:49 PM
DATE MODIFIED: 12/27/2019 4:55 PM

64. Why is an iceberg, most of which is underwater, an appropriate analogy for the consequences of a cyberattack?

a. most large businesses conceal the effects of cyberattacks from the public
b. most people only think of the direct impact of the attack, not the many other, oft-hidden effects
c. most of the consequences of a cyberattack cannot be assessed in terms of costs to a business
d. An iceberg is not an appropriate analogy for the consequences of a cyberattack.

ANSWER: b
RATIONALE: The image of the iceberg is appropriate for a discussion of the successful consequences of a cyberattack because most people only think of the direct impact of a successful cyberattack and do not consider all the other oft-hidden effects.

Copyright Cengage Learning. Powered by Cognero.

FEEDBACK:

a. The image of the iceberg is appropriate for a discussion of the successful consequences of a cyberattack because most people only think of the direct impact of a successful cyberattack and do not consider all the other oft-hidden effects.
b. The image of the iceberg is appropriate for a discussion of the successful consequences of a cyberattack because most people only think of the direct impact of a successful cyberattack and do not consider all the other oft-hidden effects.
c. The image of the iceberg is appropriate for a discussion of the successful consequences of a cyberattack because most people only think of the direct impact of a successful cyberattack and do not consider all the other oft-hidden effects.
d. The image of the iceberg is appropriate for a discussion of the successful consequences of a cyberattack because most people only think of the direct impact of a successful cyberattack and do not consider all the other oft-hidden effects.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Consequences of a Successful Cyberattack
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.6 - Identify five consequences of a successful cyberattack.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/28/2019 3:36 PM
DATE MODIFIED: 12/28/2019 4:01 PM

65. A health insurance firm is hit by a successful cyberattack. The value of the assets stolen or damaged due to the cyberattack is considered _____.

a. the direct impact of the cyberattack
b. the business disruption caused by the cyberattack
c. the recovery cost of the cyberattack
d. the legal consequences of the cyberattack

ANSWER: a
RATIONALE: The direct impact of a cyberattack is the value of the assets (cash, inventory, equipment, patents, copyrights, trade secrets, data) stolen or damaged due to the cyberattack. Shareholders of the organizations will also experience a direct impact from the drop in the share price that typically follows a major cyberattack.

FEEDBACK:

a. The direct impact of a cyberattack is the value of the assets (cash, inventory, equipment, patents, copyrights, trade secrets, data) stolen or damaged due to the cyberattack.
b. The direct impact of a cyberattack is the value of the assets (cash, inventory, equipment, patents, copyrights, trade secrets, data) stolen or damaged due to the cyberattack.
c. The direct impact of a cyberattack is the value of the assets (cash, inventory, equipment, patents, copyrights, trade secrets, data) stolen or damaged due to the cyberattack.
d. The direct impact of a cyberattack is the value of the assets (cash, inventory, equipment, patents, copyrights, trade secrets, data) stolen or damaged due to the cyberattack.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Consequences of a Successful Cyberattack

Copyright Cengage Learning. Powered by Cognero.

QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.6 - Identify five consequences of a successful cyberattack.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/28/2019 4:03 PM
DATE MODIFIED: 12/28/2019 4:22 PM

66. After a successful cyberattack on its information systems, a toy manufacturer is unable to operate effectively for two weeks, and thus misses out on some significant customer orders during this time owing to _____.

a. business disruption
b. recovery costs
c. legal obligations
d. reputation damage

ANSWER: a
RATIONALE: A successful cyberattack may make it impossible for the organization to operate in an effective manner for several hours or days. This business disruption can cause a loss of existing business and customers as well as the loss of potential new business and customers. In addition, resources may be diverted from their regular duties to scramble to operate some sort of back-up procedures that enables essential business processes to continue—albeit at a lower level of efficiency.
FEEDBACK:
a. A successful cyberattack may make it impossible for the organization to operate in an effective manner for several hours or days. This business disruption can cause a loss of existing business and customers as well as the loss of potential new business and customers.
b. A successful cyberattack may make it impossible for the organization to operate in an effective manner for several hours or days. This business disruption can cause a loss of existing business and customers as well as the loss of potential new business and customers.
c. A successful cyberattack may make it impossible for the organization to operate in an effective manner for several hours or days. This business disruption can cause a loss of existing business and customers as well as the loss of potential new business and customers.
d. A successful cyberattack may make it impossible for the organization to operate in an effective manner for several hours or days. This business disruption can cause a loss of existing business and customers as well as the loss of potential new business and customers.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Consequences of a Successful Cyberattack
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.6 - Identify five consequences of a successful cyberattack.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/28/2019 4:24 PM
DATE MODIFIED: 12/28/2019 4:51 PM

67. Violating the European Union General Data Protection Regulation guidelines will most likely increase a successful

Copyright Cengage Learning. Powered by Cognero.

cyberattack's _____.

a. direct impacts
b. recovery costs
c. legal consequences
d. reputation damage

ANSWER: c

RATIONALE: Legal consequences of cyberattacks include the prospect of monetary penalties for businesses that fail to comply with data protection legislation. For example, the European Union General Data Protection Regulation (GDPR) has established strong guidelines for how organizations process and handle data so that the personal information of individuals is protected. Organizations that violate these guidelines can be fined 20 million euros ($23 million U.S. dollars), or 4 percent of global annual revenue—whichever is greater.

FEEDBACK:

a. Legal consequences of cyberattacks include the prospect of monetary penalties for businesses that fail to comply with data protection legislation. For example, the European Union General Data Protection Regulation (GDPR) has established strong guidelines for how organizations process and handle data so that the personal information of individuals is protected.
b. Legal consequences of cyberattacks include the prospect of monetary penalties for businesses that fail to comply with data protection legislation. For example, the European Union General Data Protection Regulation (GDPR) has established strong guidelines for how organizations process and handle data so that the personal information of individuals is protected.
c. Legal consequences of cyberattacks include the prospect of monetary penalties for businesses that fail to comply with data protection legislation. For example, the European Union General Data Protection Regulation (GDPR) has established strong guidelines for how organizations process and handle data so that the personal information of individuals is protected.
d. Legal consequences of cyberattacks include the prospect of monetary penalties for businesses that fail to comply with data protection legislation. For example, the European Union General Data Protection Regulation (GDPR) has established strong guidelines for how organizations process and handle data so that the personal information of individuals is protected.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Consequences of a Successful Cyberattack
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.6 - Identify five consequences of a successful cyberattack.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/28/2019 4:52 PM
DATE MODIFIED: 12/28/2019 4:59 PM

68. The percentage of adults in an area who are interested in opening an account with an investment company drops significantly after the media reports on a successful cyberattack on this organization. This is most likely the result of _____.

a. the direct impact of the cyberattack
b. recovery procedures followed after the cyberattack
c. legal ramifications of the cyberattack

Copyright Cengage Learning. Powered by Cognero.

d. reputation damage related to the cyberattack

ANSWER: d

RATIONALE: A successful cyberattack can erode the trust your organization has established with your customers, suppliers, business partners, and shareholders. This damage to your organization's reputation leads to a devaluation of the products and services of your organization resulting in a drop in stock price, loss of customers, supplier turnover, strained business partner relationships, and ultimately, a loss of sales and decrease in profits.

FEEDBACK:

a. Damage to your organization's reputation following a cyberattack leads to a devaluation of the products and services of your organization resulting in a drop in stock price, loss of customers, supplier turnover, strained business partner relationships, and ultimately, a loss of sales and decrease in profits.

b. Damage to your organization's reputation following a cyberattack leads to a devaluation of the products and services of your organization resulting in a drop in stock price, loss of customers, supplier turnover, strained business partner relationships, and ultimately, a loss of sales and decrease in profits.

c. Damage to your organization's reputation following a cyberattack leads to a devaluation of the products and services of your organization resulting in a drop in stock price, loss of customers, supplier turnover, strained business partner relationships, and ultimately, a loss of sales and decrease in profits.

d. Damage to your organization's reputation following a cyberattack leads to a devaluation of the products and services of your organization resulting in a drop in stock price, loss of customers, supplier turnover, strained business partner relationships, and ultimately, a loss of sales and decrease in profits.

POINTS: 1

DIFFICULTY: Easy

REFERENCES: Consequences of a Successful Cyberattack

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

LEARNING OBJECTIVES: POIS.14e.2.6 - Identify five consequences of a successful cyberattack.

KEYWORDS: Bloom's: Remember

DATE CREATED: 12/28/2019 5:01 PM

DATE MODIFIED: 12/28/2019 5:08 PM

69. After a successful cyberattack, the funds spent on repairing affected systems, restoring lost data, and performing a post-incident analysis are considered part of the _____.

a. direct impact

b. business disruption

c. recovery cost

d. legal consequences

ANSWER: c

RATIONALE: Cyberattacks may entail significant recovery costs. It may take people from the IS organization and business areas days or weeks to repair affected systems and recover lost or compromised data. Resources will need to be drawn from their normal work responsibilities to perform a post-incident analysis to identify the scope, cause, and impact of the cyberattack and to determine measures to prevent a reoccurrence.

FEEDBACK:

a. Cyberattacks may entail significant recovery costs. It may take people from the IS organization and business areas days or weeks to repair affected systems and recover lost or compromised data. Resources will need to be drawn from their normal work

responsibilities to perform a post-incident analysis.

b. Cyberattacks may entail significant recovery costs. It may take people from the IS organization and business areas days or weeks to repair affected systems and recover lost or compromised data. Resources will need to be drawn from their normal work responsibilities to perform a post-incident analysis.

c. Cyberattacks may entail significant recovery costs. It may take people from the IS organization and business areas days or weeks to repair affected systems and recover lost or compromised data. Resources will need to be drawn from their normal work responsibilities to perform a post-incident analysis.

d. Cyberattacks may entail significant recovery costs. It may take people from the IS organization and business areas days or weeks to repair affected systems and recover lost or compromised data. Resources will need to be drawn from their normal work responsibilities to perform a post-incident analysis.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Consequences of a Successful Cyberattack
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.6 - Identify five consequences of a successful cyberattack.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/28/2019 5:11 PM
DATE MODIFIED: 12/28/2019 5:18 PM

70. Legal consequences following a successful cyberattack on a well-known organization often include _____.

a. the loss of cash, inventory, equipment, patents, copyrights, trade secrets, and data
b. the diversion of resources to the operation of back-up procedures
c. lawsuits initiated by consumers who incurred damages
d. an erosion of trust previously established with customers, suppliers, and partners

ANSWER: c
RATIONALE: Consumers are almost certain to initiate lawsuits to recover any damages incurred from a cyberattack. Many organizations that suffer a cyberattack that compromises the personal data of employees, customers, or patients provide one or two years of identity theft insurance or consumer credit monitoring for those impacted.
FEEDBACK:

a. Consumers are almost certain to initiate lawsuits to recover any damages incurred from a cyberattack.

b. Consumers are almost certain to initiate lawsuits to recover any damages incurred from a cyberattack.

c. Consumers are almost certain to initiate lawsuits to recover any damages incurred from a cyberattack.

d. Consumers are almost certain to initiate lawsuits to recover any damages incurred from a cyberattack.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Consequences of a Successful Cyberattack
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.6 - Identify five consequences of a successful cyberattack.

Copyright Cengage Learning. Powered by Cognero.

TIVES:
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/28/2019 5:23 PM
DATE MODIFIED: 12/28/2019 5:32 PM

71. Thanks to the Identity Theft and Assumption Deterrence Act, _____.
   a. identity theft is a federal crime for which perpetrators may be sentenced to up to 15 years in prison.
   b. the definition of and legal penalties for identity theft are determined at the state government level.
   c. the maximum term of imprisonment for convicted identity thieves is the same as for cyberterrorists.
   d. identity theft has become much less common and is no longer a major security threat.

ANSWER: a
RATIONALE: The Identity Theft and Assumption Deterrence Act (U.S. Code Title 18, Section 1028) makes identity theft a federal crime, with penalties of up to 15 years of imprisonment and a maximum fine of $250,000. Those convicted of cyberterrorism are subject to a prison term of 5–20 years.
FEEDBACK:
   a. The Identity Theft and Assumption Deterrence Act makes identity theft a federal crime, with penalties of up to 15 years of imprisonment and a maximum fine of $250,000.
   b. The Identity Theft and Assumption Deterrence Act makes identity theft a federal crime, with penalties of up to 15 years of imprisonment and a maximum fine of $250,000.
   c. The Identity Theft and Assumption Deterrence Act makes identity theft a federal crime, with penalties of up to 15 years of imprisonment and a maximum fine of $250,000.
   d. The Identity Theft and Assumption Deterrence Act makes identity theft a federal crime, with penalties of up to 15 years of imprisonment and a maximum fine of $250,000.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Federal Laws for Prosecuting Computer Attacks
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.7 - Identify five federal laws that address computer crime.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/29/2019 4:11 PM
DATE MODIFIED: 12/29/2019 4:24 PM

72. While conducting a security self-assessment of his personal laptop use, Vann realizes that he is putting himself at risk by _____.
   a. upgrading his operating system too often
   b. installing both firewall and antivirus software at the same time
   c. purchasing new anti-malware software before it has been reviewed by other consumers
   d. putting off installing available software updates that he has been notified about

ANSWER: d
RATIONALE: According to the self-assessment security test in Table 2.6, you are minimizing your risk of cyberattack at the end-user level if you do the following:

- have the most current version of your computer's operating system installed
- have the most current version of firewall, antivirus, and malware software installed
- install updates to all your software when you receive notice that a new update is available

Copyright Cengage Learning. Powered by Cognero.

FEEDBACK:

a. According to the self-assessment security test in Table 2.6, you should have the most current version of your computer's operating system installed; have the most current version of firewall, antivirus, and malware software installed; and install updates to all your software when you receive notice that a new update is available.

b. According to the self-assessment security test in Table 2.6, you should have the most current version of your computer's operating system installed; have the most current version of firewall, antivirus, and malware software installed; and install updates to all your software when you receive notice that a new update is available.

c. According to the self-assessment security test in Table 2.6, you should have the most current version of your computer's operating system installed; have the most current version of firewall, antivirus, and malware software installed; and install updates to all your software when you receive notice that a new update is available.

d. According to the self-assessment security test in Table 2.6, you should have the most current version of your computer's operating system installed; have the most current version of firewall, antivirus, and malware software installed; and install updates to all your software when you receive notice that a new update is available.

POINTS: 1

DIFFICULTY: Easy

REFERENCES: Implementing CIA at the End-User Level

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

LEARNING OBJECTIVES: POIS.14e.2.9 - Conduct a security self-assessment of your own computer and usage habits.

KEYWORDS: Bloom's: Understand

DATE CREATED: 12/29/2019 4:28 PM

DATE MODIFIED: 12/29/2019 4:39 PM

73. Imagine you are conducting a security self-assessment. Which of the following might indicate one of your account passwords is too weak?

a. it includes a mixture of capital and lower-case letters
b. it includes several special characters
c. it contains fewer than 12 characters
d. it contains numbers as well as letters

ANSWER: c

RATIONALE: According to the self-assessment security test in Table 2.6, you should use different, strong passwords for each of your accounts and applications—a minimum of 12 characters, with a mix of capital and lowercase letters, numbers, and special characters.

FEEDBACK:

a. According to the self-assessment security test in Table 2.6, you should use different, strong passwords for each of your accounts and applications—a minimum of 12 characters, with a mix of capital and lowercase letters, numbers, and special characters.

b. According to the self-assessment security test in Table 2.6, you should use different, strong passwords for each of your accounts and applications—a minimum of 12 characters, with a mix of capital and lowercase letters, numbers, and special characters.

c. According to the self-assessment security test in Table 2.6, you should use different, strong passwords for each of your accounts and applications—a minimum of 12 characters, with a mix of capital and lowercase letters, numbers, and special characters.

d. According to the self-assessment security test in Table 2.6, you should use different,

Copyright Cengage Learning. Powered by Cognero.

strong passwords for each of your accounts and applications—a minimum of 12 characters, with a mix of capital and lowercase letters, numbers, and special characters.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the End-User Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.9 - Conduct a security self-assessment of your own computer and usage habits.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/29/2019 5:04 PM
DATE MODIFIED: 12/29/2019 5:13 PM

74. Which of the following choices will help you score better (that is, as more secure) on a security self-assessment?
    a. accessing corporate applications directly rather than via a VPN
    b. setting your home wireless router's encryption method to WPA2
    c. utilizing the default name and password on your home wireless router
    d. checking email while using a free, public wireless network

ANSWER: b

RATIONALE: According to the self-assessment security test in Table 2.6, you are minimizing your risk of cyberattack at the end-user level if you do the following:

- become familiar with and follow your organization's policies for accessing corporate Web sites and applications from your home or remote locations (e.g., access via a VPN)
- set the encryption method to WPA2 and changed the default name and password on your home wireless router
- when using a free, public wireless network, avoid checking your email or accessing Web sites requiring a username and password

FEEDBACK:

a. According to the self-assessment security test in Table 2.6, you should become familiar with and follow your organization's policies for accessing corporate Web sites and applications from your home or remote locations (e.g., access via a VPN); set the encryption method to WPA2 and changed the default name and password on your home wireless router; and when using a free, public wireless network, avoid checking your email or accessing Web sites requiring a username and password.

b. According to the self-assessment security test in Table 2.6, you should become familiar with and follow your organization's policies for accessing corporate Web sites and applications from your home or remote locations (e.g., access via a VPN); set the encryption method to WPA2 and changed the default name and password on your home wireless router; and when using a free, public wireless network, avoid checking your email or accessing Web sites requiring a username and password.

c. According to the self-assessment security test in Table 2.6, you should become familiar with and follow your organization's policies for accessing corporate Web sites and applications from your home or remote locations (e.g., access via a VPN); set the encryption method to WPA2 and changed the default name and password on your home wireless router; and when using a free, public wireless network, avoid checking your email or accessing Web sites requiring a username and password.

d. According to the self-assessment security test in Table 2.6, you should become familiar with and follow your organization's policies for accessing corporate Web sites and applications from your home or remote locations (e.g., access via a VPN); set the

Copyright Cengage Learning. Powered by Cognero.

encryption method to WPA2 and changed the default name and password on your home wireless router; and when using a free, public wireless network, avoid checking your email or accessing Web sites requiring a username and password.

POINTS: 1
DIFFICULTY: Moderate
REFERENCES: Implementing CIA at the End-User Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.9 - Conduct a security self-assessment of your own computer and usage habits.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/29/2019 5:16 PM
DATE MODIFIED: 12/29/2019 5:24 PM

75. A security self-assessment revealed that Penelope, who owns one laptop computer, is putting herself at risk for cyberattack by _____.

a. avoiding signing in to her Amazon.com account while using free wifi at the coffee shop
b. deleting emails from people or businesses unfamiliar to her
c. refraining from clicking on URLs in the bodies of email messages
d. backing up critical files to a single folder on her laptop once every three months

ANSWER: d
RATIONALE: According to the self-assessment security test in Table 2.6, you are minimizing your risk of cyberattack at the end-user level if you do the following:

- when using a free, public wireless network, avoid checking your email or accessing Web sites requiring a username and password
- refrain from clicking on a URL in an email from someone you do not know
- back up critical files to a separate device at least once a week

FEEDBACK:

a. According to the self-assessment security test in Table 2.6, you should refrain from clicking on a URL in an email from someone you do not know; back up critical files to a separate device at least once a week; and, when using a free, public wireless network, avoid checking your email or accessing Web sites requiring a username and password.
b. According to the self-assessment security test in Table 2.6, you should refrain from clicking on a URL in an email from someone you do not know; back up critical files to a separate device at least once a week; and, when using a free, public wireless network, avoid checking your email or accessing Web sites requiring a username and password.
c. According to the self-assessment security test in Table 2.6, you should refrain from clicking on a URL in an email from someone you do not know; back up critical files to a separate device at least once a week; and, when using a free, public wireless network, avoid checking your email or accessing Web sites requiring a username and password.
d. According to the self-assessment security test in Table 2.6, you should refrain from clicking on a URL in an email from someone you do not know; back up critical files to a separate device at least once a week; and, when using a free, public wireless network, avoid checking your email or accessing Web sites requiring a username and password.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the End-User Level
QUESTION TYPE: Multiple Choice

Copyright Cengage Learning. Powered by Cognero.

HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.9 - Conduct a security self-assessment of your own computer and usage habits.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/29/2019 5:26 PM
DATE MODIFIED: 12/29/2019 5:34 PM

76. To improve his score on a security self-assessment, Saul set up his laptop so that the first thing he must do when he turns it on is _____.

a. install new software updates
b. log in to his employer's VPN
c. enter a strong security password
d. run a file backup procedure

ANSWER: c
RATIONALE: According to the self-assessment security test in Table 2.6, you should arm your device with a security passcode that must be entered before it accepts further input.
FEEDBACK:
a. According to the self-assessment security test in Table 2.6, you should arm your device with a security passcode that must be entered before it accepts further input.
b. According to the self-assessment security test in Table 2.6, you should arm your device with a security passcode that must be entered before it accepts further input.
c. According to the self-assessment security test in Table 2.6, you should arm your device with a security passcode that must be entered before it accepts further input.
d. According to the self-assessment security test in Table 2.6, you should arm your device with a security passcode that must be entered before it accepts further input.
POINTS: 1
DIFFICULTY: Moderate
REFERENCES: Implementing CIA at the End-User Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.9 - Conduct a security self-assessment of your own computer and usage habits.
KEYWORDS: Bloom's: Understand
DATE CREATED: 12/29/2019 5:35 PM
DATE MODIFIED: 12/29/2019 5:40 PM

77. When Tiffany takes a security self-assessment, she discovers that she is increasing her risk of a cyberattack by _____.

a. leaving her tablet computer unattended at the bistro table while she purchases her lunch at the counter
b. installing Locate My Device or a similar program that she downloaded online
c. following her employer's policies regarding personal data storage
d. accessing database applications from her home computer via a VPN

ANSWER: a
RATIONALE: According to the self-assessment security test in Table 2.6, you are minimizing your risk of cyberattack at the end-user level if you do the following:

- become familiar with and follow your organization’s policies for accessing corporate Web sites and applications from your home or remote locations (e.g., access via a VPN)
- become familiar with and follow your organization’s policies regarding the storage of

personal or confidential data on your device
- install Locate My Device or similar software in case your device is lost or stolen
- make sure not to leave your device unattended in a public place where it can be easily stolen

FEEDBACK:

a. According to the self-assessment security test in Table 2.6, you should install Locate My Device or similar software in case your device is lost or stolen and make sure not to leave your device unattended in a public place where it can be easily stolen.

b. According to the self-assessment security test in Table 2.6, you should install Locate My Device or similar software in case your device is lost or stolen and make sure not to leave your device unattended in a public place where it can be easily stolen.

c. According to the self-assessment security test in Table 2.6, you should install Locate My Device or similar software in case your device is lost or stolen and make sure not to leave your device unattended in a public place where it can be easily stolen.

d. According to the self-assessment security test in Table 2.6, you should install Locate My Device or similar software in case your device is lost or stolen and make sure not to leave your device unattended in a public place where it can be easily stolen.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the End-User Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.9 - Conduct a security self-assessment of your own computer and usage habits.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/30/2019 6:40 AM
DATE MODIFIED: 12/30/2019 6:50 AM

78. After completing a security self-assessment, Hal decides to improve his practices related to use of social media sites such as Facebook. How can he make his social media use safer?

a. access social media sites via a VPN
b. change his password to one that includes only numbers and is eight characters long
c. review, understand, and if necessary adjust his privacy settings for these sites
d. run his antivirus software just before he logs in to these sites

ANSWER: c
RATIONALE: According to the self-assessment security test in Table 2.6, you should review, and ensure you understand, the privacy settings that control who can see or read what you do on Facebook and other social media sites. VPNs are security measures used when accessing corporate Web sites and applications from home or remote locations. Running antivirus software is useful, but doing so before visiting a social media site will be less helpful than adjusting the privacy settings.

FEEDBACK:

a. According to the self-assessment security test in Table 2.6, you should review, and ensure you understand, the privacy settings that control who can see or read what you do on Facebook and other social media sites.

b. According to the self-assessment security test in Table 2.6, you should review, and ensure you understand, the privacy settings that control who can see or read what you do on Facebook and other social media sites.

c. According to the self-assessment security test in Table 2.6, you should review, and ensure you understand, the privacy settings that control who can see or read what you do on Facebook and other social media sites.

Copyright Cengage Learning. Powered by Cognero.

d. According to the self-assessment security test in Table 2.6, you should review, and ensure you understand, the privacy settings that control who can see or read what you do on Facebook and other social media sites.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the End-User Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.9 - Conduct a security self-assessment of your own computer and usage habits.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/30/2019 6:51 AM
DATE MODIFIED: 12/30/2019 7:02 AM

79. The first two steps an organization must take to perform a security risk assessment are to identify _____, respectively.
a. the impact and frequency of each possible loss event
b. the costs of each possible loss event and the benefits of investing resources to prevent each
c. the current protections against cyberattacks that are already in place and the least expensive ways to upgrade or expand them
d. hardware, software, and information systems used to achieve business objectives and possible occurrences that would negatively impact them

ANSWER: d
RATIONALE: The goal of risk assessment is to identify which investments of time and resources will best protect the organization from its most likely and serious threats. In the context of an IT risk assessment, an asset is any hardware, software, information system, network, or database that is used by the organization to achieve its business objectives. A loss event is any occurrence that has a negative impact on an asset. Examples of loss events include a computer contracting a virus or a Web site undergoing a DDoS attack.

The first two steps in a general security risk assessment process are as follows:

- Step 1—Identify the set of IT assets about which the organization is most concerned. Priority is typically given to those assets that support the organization's mission and the meeting of its primary business goals.
- Step 2—Identify the loss events or the risks or threats that could occur, such as a DDoS attack or insider fraud.

FEEDBACK:
a. The first two steps in a general security risk assessment process are as follows: Step 1—Identify the set of IT assets about which the organization is most concerned. Priority is typically given to those assets that support the organization's mission and the meeting of its primary business goals. Step 2—Identify the loss events or the risks or threats that could occur, such as a DDoS attack or insider fraud.
b. The first two steps in a general security risk assessment process are as follows: Step 1—Identify the set of IT assets about which the organization is most concerned. Priority is typically given to those assets that support the organization's mission and the meeting of its primary business goals. Step 2—Identify the loss events or the risks or threats that could occur, such as a DDoS attack or insider fraud.
c. The first two steps in a general security risk assessment process are as follows: Step 1—Identify the set of IT assets about which the organization is most concerned. Priority is typically given to those assets that support the organization's mission and the

Copyright Cengage Learning. Powered by Cognero.

meeting of its primary business goals. Step 2—Identify the loss events or the risks or threats that could occur, such as a DDoS attack or insider fraud.

d. The first two steps in a general security risk assessment process are as follows: Step 1 —Identify the set of IT assets about which the organization is most concerned. Priority is typically given to those assets that support the organization's mission and the meeting of its primary business goals. Step 2—Identify the loss events or the risks or threats that could occur, such as a DDoS attack or insider fraud.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the Organizational Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.10 - Identify eight steps that must be taken to perform a thorough security risk assessment.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/30/2019 7:06 AM
DATE MODIFIED: 12/30/2019 9:56 AM

80. Because some threats, such as insider fraud, are more likely to occur than others, step 3 of the risk assessment process is to _____.

a. identify the set of IT assets about which the organization is most concerned
b. assess the frequency of events or the likelihood of each potential threat
c. perform a cost-benefit analysis to ensure that your efforts will be cost effective
d. determine how each threat can be mitigated so it becomes less likely to occur

ANSWER: b
RATIONALE: The third step in a general security risk assessment process is as follows: Step 3—Assess the frequency of events or the likelihood of each potential threat; some threats, such as insider fraud, are more likely to occur than others.
FEEDBACK:

a. The third step in a general security risk assessment process is as follows: Step 3—Assess the frequency of events or the likelihood of each potential threat.
b. The third step in a general security risk assessment process is as follows: Step 3—Assess the frequency of events or the likelihood of each potential threat.
c. The third step in a general security risk assessment process is as follows: Step 3—Assess the frequency of events or the likelihood of each potential threat.
d. The third step in a general security risk assessment process is as follows: Step 3—Assess the frequency of events or the likelihood of each potential threat.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the Organizational Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.10 - Identify eight steps that must be taken to perform a thorough security risk assessment.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/30/2019 2:27 PM
DATE MODIFIED: 12/30/2019 2:31 PM

Copyright Cengage Learning. Powered by Cognero.

81. Eboni is part of a workgroup conducting a security risk assessment at her firm and is currently helping to determine the impact of each threat they have identified, should it occur. Because a later step in the assessment process involves performing a cost-benefit analysis, Eboni will include _____.

a. the estimated cost of the direct impact, business disruption, recovery efforts, and legal and reputation damages
b. a documented process for recovering an organization's business information system assets
c. a document that includes an organization's disaster recovery plan, continuity of operations plan, and incident management plan
d. reasonable assurance that the cost of control does not exceed the system's benefits or the risks involved

ANSWER: a

RATIONALE: The fourth step in a general security risk assessment process is as follows: Step 4—Determine the impact of each threat occurring. Would the threat have a minor impact on the organization, or could it keep the organization from carrying out its mission for a lengthy period of time? Step 7 is to perform a cost-benefit analysis to ensure that your efforts will be cost effective. Table 2.4 illustrates a risk assessment for a hypothetical organization. The estimated cost includes the cost of the direct impact, the business disruption, the recovery efforts, and the legal and reputational damage.

FEEDBACK:

a. The fourth step in a general security risk assessment process is as follows: Step 4—Determine the impact of each threat occurring. The estimated cost used in the cost-benefit analysis in step 7 includes the cost of the direct impact, the business disruption, the recovery efforts, and the legal and reputational damage.
b. The fourth step in a general security risk assessment process is as follows: Step 4—Determine the impact of each threat occurring. The estimated cost used in the cost-benefit analysis in step 7 includes the cost of the direct impact, the business disruption, the recovery efforts, and the legal and reputational damage.
c. The fourth step in a general security risk assessment process is as follows: Step 4—Determine the impact of each threat occurring. The estimated cost used in the cost-benefit analysis in step 7 includes the cost of the direct impact, the business disruption, the recovery efforts, and the legal and reputational damage.
d. The fourth step in a general security risk assessment process is as follows: Step 4—Determine the impact of each threat occurring. The estimated cost used in the cost-benefit analysis in step 7 includes the cost of the direct impact, the business disruption, the recovery efforts, and the legal and reputational damage.

POINTS: 1
DIFFICULTY: Moderate
REFERENCES: Implementing CIA at the Organizational Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.10 - Identify eight steps that must be taken to perform a thorough security risk assessment.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/30/2019 2:33 PM
DATE MODIFIED: 12/30/2019 2:48 PM

82. Steps 5 and 6 of the security risk assessment process are to determine the possible ways to accomplish a key task and how feasible each option would be to implement. What is that task?

a. threat mitigation
b. asset replacement
c. event identification
d. cost-benefit analysis

Copyright Cengage Learning. Powered by Cognero.

ANSWER: a

RATIONALE: The goal of risk assessment is to identify which investments of time and resources will best protect the organization from its most likely and serious threats. In the context of an IT risk assessment, an asset is any hardware, software, information system, network, or database that is used by the organization to achieve its business objectives. A loss event is any occurrence that has a negative impact on an asset. Examples of loss events include a computer contracting a virus or a Web site undergoing a DDoS attack.

The fifth and sixth steps in a general security risk assessment process are as follows:

- Step 5—Determine how each threat can be mitigated so that it becomes much less likely to occur or, if it does occur, has less of an impact on the organization. For example, installing virus protection on all computers makes it much less likely that a computer will contract a virus. Due to time and resource limitations, most organizations choose to focus on just those threats that have a high (relative to all other threats) probability of occurrence and a high (relative to all other threats) impact. In other words, first address those threats that are likely to occur and that would have a high negative impact on the organization.
- Step 6—Assess the feasibility of implementing the mitigation options.

FEEDBACK:

a. The fifth and sixth steps in a general security risk assessment process are as follows: Step 5—Determine how each threat can be mitigated so that it becomes much less likely to occur or, if it does occur, has less of an impact on the organization. Step 6—Assess the feasibility of implementing the mitigation options.

b. The fifth and sixth steps in a general security risk assessment process are as follows: Step 5—Determine how each threat can be mitigated so that it becomes much less likely to occur or, if it does occur, has less of an impact on the organization. Step 6—Assess the feasibility of implementing the mitigation options.

c. The fifth and sixth steps in a general security risk assessment process are as follows: Step 5—Determine how each threat can be mitigated so that it becomes much less likely to occur or, if it does occur, has less of an impact on the organization. Step 6—Assess the feasibility of implementing the mitigation options.

d. The fifth and sixth steps in a general security risk assessment process are as follows: Step 5—Determine how each threat can be mitigated so that it becomes much less likely to occur or, if it does occur, has less of an impact on the organization. Step 6—Assess the feasibility of implementing the mitigation options.

POINTS: 1

DIFFICULTY: Moderate

REFERENCES: Implementing CIA at the Organizational Level

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

LEARNING OBJECTIVES: POIS.14e.2.10 - Identify eight steps that must be taken to perform a thorough security risk assessment.

KEYWORDS: Bloom's: Remember

DATE CREATED: 12/30/2019 2:50 PM

DATE MODIFIED: 12/30/2019 2:58 PM

83. Kenneth is assisting with step 7 of his organization's security risk assessment. He and his team compare the risks of potential security breaches against the estimated costs of preventing them from happening. Why is this an important step?

a. Data availability requires implementing products, services, policies, and procedures to ensure that data are accessible.

b. Periodic security audits are needed to ensure that individuals are following established policies.

Copyright Cengage Learning. Powered by Cognero.

c. No amount of resources can guarantee a perfect security system, so one must balance risks with prevention costs.

d. Taking action to prevent cyberattacks, such as installing protective software, makes them much less likely to occur.

ANSWER: c

RATIONALE: Step 7 is to perform a cost-benefit analysis to ensure that your efforts will be cost effective. No amount of resources can guarantee a perfect security system, so organizations must balance the risk of a security breach with the cost of preventing one.

FEEDBACK:

a. Step 7 is to perform a cost-benefit analysis to ensure that your efforts will be cost effective. No amount of resources can guarantee a perfect security system, so organizations must balance the risk of a security breach with the cost of preventing one.

b. Step 7 is to perform a cost-benefit analysis to ensure that your efforts will be cost effective. No amount of resources can guarantee a perfect security system, so organizations must balance the risk of a security breach with the cost of preventing one.

c. Step 7 is to perform a cost-benefit analysis to ensure that your efforts will be cost effective. No amount of resources can guarantee a perfect security system, so organizations must balance the risk of a security breach with the cost of preventing one.

d. Step 7 is to perform a cost-benefit analysis to ensure that your efforts will be cost effective. No amount of resources can guarantee a perfect security system, so organizations must balance the risk of a security breach with the cost of preventing one.

POINTS: 1

DIFFICULTY: Easy

REFERENCES: Implementing CIA at the Organizational Level

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

LEARNING OBJECTIVES: POIS.14e.2.10 - Identify eight steps that must be taken to perform a thorough security risk assessment.

KEYWORDS: Bloom's: Remember

DATE CREATED: 12/30/2019 3:00 PM

DATE MODIFIED: 12/30/2019 3:13 PM

84. The final step in the security risk assessment process is to _____.

a. analyze the costs and benefits of various countermeasures

b. decide whether or not to implement particular countermeasures

c. create a chart that identifies loss events, their frequency, and their monetary costs

d. assess the feasibility of implementing each of the identified mitigation measures

ANSWER: b

RATIONALE: Step 8 is to make the decision on whether or not to implement a particular countermeasure. If you decide against implementing a particular countermeasure, you need to reassess if the threat is truly serious and, if so, identify a less costly countermeasure.

FEEDBACK:

a. Step 8 is to make the decision on whether or not to implement a particular countermeasure.

b. Step 8 is to make the decision on whether or not to implement a particular countermeasure.

Copyright Cengage Learning. Powered by Cognero.

c. Step 8 is to make the decision on whether or not to implement a particular countermeasure.
d. Step 8 is to make the decision on whether or not to implement a particular countermeasure.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Implementing CIA at the Organizational Level
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.10 - Identify eight steps that must be taken to perform a thorough security risk assessment.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/30/2019 3:15 PM
DATE MODIFIED: 12/30/2019 3:19 PM

85. What do AT&T, Computer Sciences Corporation, Dell SecureWorks, IBM, Symantec, and Verizon have in common?
a. they recently suffered massive data breaches
b. they pioneered bring your own device policies
c. they have reduced their security risk to zero
d. they are managed security service providers

ANSWER: d
RATIONALE: Managed security service providers (MSSPs) include such companies as AT&T, Computer Sciences Corporation, Dell SecureWorks, IBM, Symantec, and Verizon.
FEEDBACK:
a. Managed security service providers (MSSPs) include such companies as AT&T, Computer Sciences Corporation, Dell SecureWorks, IBM, Symantec, and Verizon.
b. Managed security service providers (MSSPs) include such companies as AT&T, Computer Sciences Corporation, Dell SecureWorks, IBM, Symantec, and Verizon.
c. Managed security service providers (MSSPs) include such companies as AT&T, Computer Sciences Corporation, Dell SecureWorks, IBM, Symantec, and Verizon.
d. Managed security service providers (MSSPs) include such companies as AT&T, Computer Sciences Corporation, Dell SecureWorks, IBM, Symantec, and Verizon.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Using a Managed Security Service Provider (MSSP)
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.12 - Describe the role of a managed security service provider.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/30/2019 3:46 PM
DATE MODIFIED: 12/30/2019 3:49 PM

86. What is the role of an MSSP?
a. limiting the Web sites and data that employees can access
b. monitoring system and network traffic automatically
c. combining elements of law and computer science to collect IS data

Copyright Cengage Learning. Powered by Cognero.

d. monitoring, managing, and maintaining computer and network security

ANSWER: d

RATIONALE: Many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.

FEEDBACK:

a. Many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.

b. Many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.

c. Many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.

d. Many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.

POINTS: 1

DIFFICULTY: Easy

REFERENCES: Using a Managed Security Service Provider (MSSP)

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

LEARNING OBJECTIVES: POIS.14e.2.12 - Describe the role of a managed security service provider.

KEYWORDS: Bloom's: Remember

DATE CREATED: 12/30/2019 3:50 PM

DATE MODIFIED: 12/30/2019 3:57 PM

87. Why do many small and mid-sized businesses hire MSSPs?

a. unavailability of effective antivirus and firewall software

b. legal injunctions imposed following HIPAA violations

c. lack of adequate in-house network security expertise

d. need for computer forensics services during legal proceedings

ANSWER: c

RATIONALE: Keeping up with computer criminals—and with new laws and regulations—can be daunting for organizations. Criminal hackers are constantly poking and prodding, trying to breach the security defenses of organizations. Also, laws such as HIPAA, Sarbanes-Oxley, and the USA Patriot Act require businesses to prove that they are securing their data. For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations can be too costly to acquire and maintain. As a result, many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.

FEEDBACK:

a. For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations can be too costly to acquire and maintain. As a result, many organizations outsource their network security operations to a managed security service provider (MSSP).

b. For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations can be too costly to acquire and maintain. As a result, many organizations outsource their network security operations

to a managed security service provider (MSSP).

c. For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations can be too costly to acquire and maintain. As a result, many organizations outsource their network security operations to a managed security service provider (MSSP).

d. For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations can be too costly to acquire and maintain. As a result, many organizations outsource their network security operations to a managed security service provider (MSSP).

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Using a Managed Security Service Provider (MSSP)
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.12 - Describe the role of a managed security service provider.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/30/2019 3:58 PM
DATE MODIFIED: 12/30/2019 4:06 PM

88. Samantha owns a small business that handles a lot of sensitive customer data and would be devastated by a data breach. Her IS department, which consists of one part-time consultant named Nikki, is overwhelmed by the number of alerts and false alarms constantly issued by her security-monitoring systems, and expresses concerns about their data security. What should Samantha do about this?

a. consider a managed security service provider
b. ask Nikki to disable the alerts and alarms
c. research different security software options
d. change her passwords more often

ANSWER: a
RATIONALE: For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations can be too costly to acquire and maintain. As a result, many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations. MSSPs provide a valuable service for IS departments drowning in reams of alerts and false alarms coming from virtual private networks (VPNs); antivirus, firewall, and intrusion detection systems; and other security-monitoring systems.
FEEDBACK:

a. For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations can be too costly to acquire and maintain. MSSPs provide a valuable service for IS departments drowning in reams of alerts and false alarms coming from security-monitoring systems.

b. For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations can be too costly to acquire and maintain. MSSPs provide a valuable service for IS departments drowning in reams of alerts and false alarms coming from security-monitoring systems.

c. For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations can be too costly to acquire and maintain. MSSPs provide a valuable service for IS departments drowning in reams of alerts and false alarms coming from security-monitoring systems.

d. For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations can be too costly to acquire and

Copyright Cengage Learning. Powered by Cognero.

maintain. MSSPs provide a valuable service for IS departments drowning in reams of alerts and false alarms coming from security-monitoring systems.

POINTS: 1
DIFFICULTY: Moderate
REFERENCES: Using a Managed Security Service Provider (MSSP)
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.12 - Describe the role of a managed security service provider.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/30/2019 4:07 PM
DATE MODIFIED: 12/30/2019 4:17 PM

89. Managed security service providers primarily help organizations keep pace with _____.

a. invoices and accounts receivable
b. cybercriminals and new laws and regulations
c. business objectives and mission-critical processes
d. market demands and customer expectations

ANSWER: b
RATIONALE: Keeping up with computer criminals—and with new laws and regulations—can be daunting for organizations. Criminal hackers are constantly poking and prodding, trying to breach the security defenses of organizations. Also, laws such as HIPAA, Sarbanes-Oxley, and the USA Patriot Act require businesses to prove that they are securing their data. For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations can be too costly to acquire and maintain. As a result, many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.
FEEDBACK:

a. Keeping up with computer criminals—and with new laws and regulations—can be daunting for organizations. As a result, many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.
b. Keeping up with computer criminals—and with new laws and regulations—can be daunting for organizations. As a result, many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.
c. Keeping up with computer criminals—and with new laws and regulations—can be daunting for organizations. As a result, many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.
d. Keeping up with computer criminals—and with new laws and regulations—can be daunting for organizations. As a result, many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations.

POINTS: 1
DIFFICULTY: Easy

Copyright Cengage Learning. Powered by Cognero.

REFERENCES: Using a Managed Security Service Provider (MSSP)
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.12 - Describe the role of a managed security service provider.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/30/2019 4:18 PM
DATE MODIFIED: 12/30/2019 4:26 PM

90. Assessing damage following a computer incident, investigating the unauthorized disclosure of corporate confidential data, and confirming or evaluating the impact of industrial espionage are tasks most appropriate for _____.

a. managed security service providers
b. computer forensics
c. the CIA security triad
d. a security dashboard

ANSWER: b
RATIONALE: A computer forensics investigation may be opened in response to a criminal investigation or civil litigation. It may also be launched for a variety of other reasons, for example, to retrace steps taken when data has been lost, assess damage following a computer incident, investigate the unauthorized disclosure of personal or corporate confidential data, or to confirm or evaluate the impact of industrial espionage.
FEEDBACK:
a. A computer forensics investigation may be launched for a variety of reasons, for example, to retrace steps taken when data has been lost, assess damage following a computer incident, investigate the unauthorized disclosure of personal or corporate confidential data, or to confirm or evaluate the impact of industrial espionage.
b. A computer forensics investigation may be launched for a variety of reasons, for example, to retrace steps taken when data has been lost, assess damage following a computer incident, investigate the unauthorized disclosure of personal or corporate confidential data, or to confirm or evaluate the impact of industrial espionage.
c. A computer forensics investigation may be launched for a variety of reasons, for example, to retrace steps taken when data has been lost, assess damage following a computer incident, investigate the unauthorized disclosure of personal or corporate confidential data, or to confirm or evaluate the impact of industrial espionage.
d. A computer forensics investigation may be launched for a variety of reasons, for example, to retrace steps taken when data has been lost, assess damage following a computer incident, investigate the unauthorized disclosure of personal or corporate confidential data, or to confirm or evaluate the impact of industrial espionage.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Computer Forensics
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.13 - Define the term computer forensics.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/30/2019 4:31 PM
DATE MODIFIED: 12/30/2019 4:40 PM

Copyright Cengage Learning. Powered by Cognero.

91. The accounting, tax, and advisory company Grant Thornton International has several IS labs around the world that employ experts who examine digital evidence for use in legal cases. Their activities are best characterized as an example of _____.

a. firewalls
b. loss event mitigation
c. computer forensics
d. risk assessment

ANSWER: c

RATIONALE: Computer forensics investigators work as a team to investigate an incident and conduct the forensic analysis using various methodologies and tools to ensure the computer network system is secure in an organization. For example, accounting, tax, and advisory company Grant Thornton International has several IS labs around the world that employ numerous forensic experts who examine digital evidence for use in legal cases.

FEEDBACK:

a. Computer forensics investigators such as those at Grant Thornton International work as a team to investigate an incident and conduct the forensic analysis using various methodologies and tools to ensure the computer network system is secure in an organization.
b. Computer forensics investigators such as those at Grant Thornton International work as a team to investigate an incident and conduct the forensic analysis using various methodologies and tools to ensure the computer network system is secure in an organization.
c. Computer forensics investigators such as those at Grant Thornton International work as a team to investigate an incident and conduct the forensic analysis using various methodologies and tools to ensure the computer network system is secure in an organization.
d. Computer forensics investigators such as those at Grant Thornton International work as a team to investigate an incident and conduct the forensic analysis using various methodologies and tools to ensure the computer network system is secure in an organization.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Computer Forensics
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.13 - Define the term computer forensics.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/30/2019 4:43 PM
DATE MODIFIED: 12/30/2019 4:49 PM

92. To successfully fight computer crime in a court of law, prosecutors and victims depend on a properly handled _____.

a. security education initiative
b. intrusion detection system
c. corporate security risk assessment
d. computer forensics investigation

ANSWER: d

RATIONALE: Proper handling of a computer forensics investigation is the key to fighting computer crime successfully in a court of law.

Copyright Cengage Learning. Powered by Cognero.

FEEDBACK:

a. Proper handling of a computer forensics investigation is the key to fighting computer crime successfully in a court of law.
b. Proper handling of a computer forensics investigation is the key to fighting computer crime successfully in a court of law.
c. Proper handling of a computer forensics investigation is the key to fighting computer crime successfully in a court of law.
d. Proper handling of a computer forensics investigation is the key to fighting computer crime successfully in a court of law.

POINTS: 1
DIFFICULTY: Easy
REFERENCES: Computer Forensics
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.13 - Define the term computer forensics.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/30/2019 4:50 PM
DATE MODIFIED: 12/30/2019 4:53 PM

93. The CCE, CISSP, CSFA, and GCFA certifications all indicate that someone has expertise in _____.

a. computer forensics
b. security risk assessment
c. corporate reputation management
d. social engineering

ANSWER: a
RATIONALE: Proper handling of a computer forensics investigation is the key to fighting computer crime successfully in a court of law. In addition, extensive training and certification increases the stature of a computer forensics investigator in a court of law. Numerous certifications relate to computer forensics, including the CCE (Certified Computer Examiner), CISSP (Certified Information Systems Security Professional), CSFA (CyberSecurity Forensic Analyst), and GCFA (Global Information Assurance Certification Certified Forensics Analyst).

FEEDBACK:

a. Numerous certifications relate to computer forensics, including the CCE (Certified Computer Examiner), CISSP (Certified Information Systems Security Professional), CSFA (CyberSecurity Forensic Analyst), and GCFA (Global Information Assurance Certification Certified Forensics Analyst).
b. Numerous certifications relate to computer forensics, including the CCE (Certified Computer Examiner), CISSP (Certified Information Systems Security Professional), CSFA (CyberSecurity Forensic Analyst), and GCFA (Global Information Assurance Certification Certified Forensics Analyst).
c. Numerous certifications relate to computer forensics, including the CCE (Certified Computer Examiner), CISSP (Certified Information Systems Security Professional), CSFA (CyberSecurity Forensic Analyst), and GCFA (Global Information Assurance Certification Certified Forensics Analyst).
d. Numerous certifications relate to computer forensics, including the CCE (Certified Computer Examiner), CISSP (Certified Information Systems Security Professional), CSFA (CyberSecurity Forensic Analyst), and GCFA (Global Information Assurance Certification Certified Forensics Analyst).

POINTS: 1
DIFFICULTY: Easy

Copyright Cengage Learning. Powered by Cognero.

REFERENCES: Computer Forensics
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: POIS.14e.2.13 - Define the term computer forensics.
KEYWORDS: Bloom's: Remember
DATE CREATED: 12/30/2019 4:58 PM
DATE MODIFIED: 12/30/2019 5:03 PM

Essay

94. You are being consulted for recommendations on software for sales report management. There are two choices. Choice #1 is a product from an industry leader that costs more than $1,000 per license per year. Choice #2 is a free, open-source software application that is free to download and install. The free software is written in a language that your programmers do not have expertise in. You may be able to convince management to hire the right programmer to install the free and open-source software. Considering the importance of data security, what solution would you recommend, and why?

ANSWER: I would recommend choosing the product from the industry leader. Since the software is from the industry leader, it is likely to have fewer vulnerabilities, and thus will be less risky. Large software development companies have the resources to quickly create and issue patches when new vulnerabilities are discovered. The open-source software may have vulnerabilities that have been discovered yet, or contributors to the software may not have the resources to respond rapidly when they become aware of new vulnerabilities. For these reasons, I would recommend the first solution —to purchase the software license from the industry leader.

RATIONALE: In computing, an exploit is an attack on an information system that takes advantage of a particular system vulnerability. Often this attack is made possible due to poor system design or implementation. Once the vulnerability is discovered, software developers create and issue a “fix,” or patch, to eliminate the problem. Note that the number of new software vulnerabilities identified in 2016 was 15,000—an average of 41 per day. Clearly, it can be difficult to keep up with all the required patches to fix these vulnerabilities.

POINTS: 1

RUBRIC:

Criteria	0 Failure	1 Below Expectations	2 Developing	3 Competent	4 Mastery
Identify the recommended software choice.					
Provide a rationale for selecting this software choice over the other option.					

DIFFICULTY: Easy
REFERENCES: Why Computer Incidents Are So Prevalent
QUESTION TYPE: Essay
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: POIS.14e.2.1 - State four reasons why computer incidents have become so prevalent.

Copyright Cengage Learning. Powered by Cognero.

NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/27/2019 2:37 PM

95. Pam, your new marketing manager, is exploring the purchase of tens of thousands of email addresses from a legitimate source for the purpose of sending product information to the masses. She has asked your opinion. Would you agree or disagree with her idea? Why or why not?

ANSWER: I would not agree with her idea to buy tens of thousands of email addresses and send mass emails to them. It will be considered spam and potentially marked as spam by the email filters. The email filters are quite sophisticated these days. Those emails may not make it to the inboxes of the intended audience. Given the general opinion that spam is not welcome, the email marketing campaign is not destined to make any net positive impact on the potential audience. In addition, having received "junk email" from our business would leave a not-so-good impression on people. They may reject any future, recipient-specific emails from our business. For these reasons, I would not agree with Pam.

RATIONALE: There are numerous types of attack vectors. One is spam, the use of email systems to send unsolicited email to large numbers of people. It could be considered unwise to associate one's organization with a technique that is commonly used for cyberattacks.

POINTS: 1

RUBRIC:

Criteria	0 Failure	1 Below Expectations	2 Developing	3 Competent	4 Mastery
State a position on the use of unsolicited emails for marketing purposes.					
Provide a rationale for the stated position using information about attack vectors.					

DIFFICULTY: Moderate
REFERENCES: Types of Attack Vectors
QUESTION TYPE: Essay
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: POIS.14e.2.3 - Define the term attack vector.
NATIONAL STANDARDS: United States - BUSPROG: Technology
KEYWORDS: Bloom's: Remember
DATE CREATED: 11/19/2019 5:58 PM
DATE MODIFIED: 12/27/2019 2:43 PM

96. You have been invited to speak to senior citizens about the Internet in general and email in particular. What topics would you choose to talk about to benefit your audience the most?

Copyright Cengage Learning. Powered by Cognero.

ANSWER: Knowing that phishing is an attack vector that exploits people's use of email, I would caution the senior citizens against phishing attacks. I would explain what phishing is and how to identify emails using this attack vector. I would show them samples of phishing emails and describe what happens if someone responds to them. I would also demonstrate how following a link from the email can lead to websites with malicious codes. I would give them some guidelines on what to do in case they become victims of phishing attacks.

I would also discuss spam, another attack vector that involves email. I would warn the senior citizens that they may receive messages from people or organizations they do not know or do not currently do business with, and that it is wise to set up a spam filter to automatically delete unsolicited messages and allow only mass messages that they have willingly signed up for into the mail program's inbox.

RATIONALE: Perpetrators of computer crimes use an attack vector to gain unauthorized access to a device or a network and to initiate a cyberattack. There are numerous types of attack vectors. One is phishing, the act of fraudulently using email to try to get the recipient to reveal personal data. Another attack vector that involves email is span, the use of email systems to send unsolicited email to large numbers of people.

POINTS: 1

RUBRIC:

Criteria	0 Failure	1 Below Expectations	2 Developing	3 Competent	4 Mastery
Identify and describe topics to be covered during a presentation on email security.					

DIFFICULTY: Moderate

REFERENCES: Types of Attack Vectors

QUESTION TYPE: Essay

HAS VARIABLES: False

STUDENT ENTRY MODE: Basic

LEARNING OBJECTIVES: POIS.14e.2.3 - Define the term attack vector.

NATIONAL STANDARDS: United States - BUSPROG: Technology

KEYWORDS: Bloom's: Remember

DATE CREATED: 11/19/2019 5:58 PM

DATE MODIFIED: 12/27/2019 2:59 PM

97. Your company has acquired Joggers PLC, a smaller company. The integration of the information systems can take up to 6 months, and until then Joggers PLC workers will continue following their policies. You have been tasked with ensuring that their IT practices will be safe and lead to a secure system. What advice would you give your manager regarding information security?

ANSWER: I would ensure Joggers' infrastructure is well protected by firewalls, antivirus software, and updated applications. I would enforce a password policy to make guessing the passwords improbable. I would recommend they institute a data backup policy to perform regular backups of all data. I would also restrict data access to that required for users' roles.

Copyright Cengage Learning. Powered by Cognero.

RATIONALE: A security policy defines an organization's security requirements, as well as the controls and sanctions needed to meet those requirements. A good security policy delineates responsibilities and the behavior expected of members of the organization. Experienced IT managers understand that users will often attempt to circumvent security policies or simply ignore them altogether. Because of that, automated system rules should mirror an organization's written policies whenever possible.

Installation of a corporate firewall is the most common security precaution taken by businesses. A firewall is a system of software, hardware, or a combination of both that stands guard between an organization's internal network and the Internet, and limits network access based on the organization's access policy. Antivirus software should be installed on each user's personal computer to scan a computer's memory and disk drives regularly for viruses. Files and databases can be protected by making a copy of all files and databases changed during the last few days or the last week, a technique called incremental backup.

Another important safeguard is to create roles and user accounts so that users have the authority to perform their responsibilities and nothing more. An effective system administrator will identify the similarities among users and create roles and user accounts associated with these groups.

POINTS: 1

RUBRIC:

Criteria	0 Failure	1 Below Expectations	2 Developing	3 Competent	4 Mastery
Explain how to implement CIA at several levels to minimize risk when new hardware, software, and users are brought into an organization.					

DIFFICULTY: Moderate

REFERENCES: The CIA Security Triad

QUESTION TYPE: Essay

HAS VARIABLES: False

STUDENT ENTRY MODE: Basic

LEARNING OBJECTIVES: POIS.14e.2.8 - Discuss how the CIA security triad can be implemented at the organization, network, application, and end user levels to safeguard against cyberattacks.

NATIONAL STANDARDS: United States - BUSPROG: Technology

KEYWORDS: Bloom's: Understand

DATE CREATED: 11/19/2019 5:58 PM

DATE MODIFIED: 12/27/2019 3:16 PM

98. You have been called in to collect information regarding a recent data breach at your organization. What specific information would you collect and for what reasons would you seek that information?

ANSWER: I would collect the information needed to write a formal incident report outlining exactly what happened (how the data breach occurred) and evaluating how the organization responded. This would include a detailed chronology of events and the impact of the incident, and in particular would identify any mistakes that led to the data breach so they will not be repeated in the future.

Specific data I would collect would include the following:

Copyright Cengage Learning. Powered by Cognero.

- IP address and name of host computer(s) involved
- The date and time when the incident was discovered
- The length of the incident
- How the incident was discovered
- The method used to gain access to the host computer
- A detailed discussion of vulnerabilities that were exploited
- A determination of whether or not the host was compromised as a result of the attack
- The nature of the data stored on the computer (customer, employee, financial, etc.)
- A determination of whether the accessed data is considered personal, private, or confidential
- The number of hours the system was down
- The overall impact on the business
- An estimate of total monetary damage from the incident
- A detailed chronology of all events associated with the incident

RATIONALE: A review should be conducted after an incident to determine exactly what happened and to evaluate how the organization responded. One approach is to write a formal incident report that includes a detailed chronology of events and the impact of the incident. This report should identify any mistakes so that they are not repeated in the future. The experience from this incident should be used to update and revise the security incident response plan. The key elements of a formal incident report should include the following:

- IP address and name of host computer(s) involved
- The date and time when the incident was discovered
- The length of the incident
- How the incident was discovered
- The method used to gain access to the host computer
- A detailed discussion of vulnerabilities that were exploited
- A determination of whether or not the host was compromised as a result of the attack
- The nature of the data stored on the computer (customer, employee, financial, etc.)
- A determination of whether the accessed data is considered personal, private, or confidential
- The number of hours the system was down
- The overall impact on the business
- An estimate of total monetary damage from the incident
- A detailed chronology of all events associated with the incident

POINTS: 1

RUBRIC:

Criteria	0 Failure	1 Below Expectations	2 Developing	3 Competent	4 Mastery
Describe the data that should be collected in response to a successful cyberattack.					
Explain how this information will be used.					

DIFFICULTY: Moderate

REFERENCES: Response

QUESTION TYPE: Essay

Copyright Cengage Learning. Powered by Cognero.

HAS VARIABLES: False

STUDENT ENTRY MODE: Basic

LEARNING OBJECTIVES: POIS.14e.2.11 - Describe five actions an organization must take in response to a successful cyberattack.

NATIONAL STANDARDS: United States - BUSPROG: Technology

KEYWORDS: Bloom's: Understand

DATE CREATED: 11/19/2019 5:58 PM

DATE MODIFIED: 12/27/2019 3:29 PM

Copyright Cengage Learning. Powered by Cognero.