Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

Chapter 1 Test Bank

Multiple-Choice Questions

1. What does the main goal of information security protect?

A. Nonpublic personally identifiable information
B. Confidentiality, integrity, and availability
C. Personal health data and biometrics
D. Financial data of public entities

Answer: B Reference: CH01, What Is Information Security?

Explanation: Information security is the study and practice of protecting information. The main goal of information security is to protect the confidentiality, integrity, and availability of information.

Type: Multiple Choice Difficulty: Medium Category: Understand

2. Which of the following is true with respect to cryptography?

A. It categorizes information to prevent unauthorized access.
B. It preserves confidentiality.
C. It is used today only by health care providers to protect health care data.
D. It ensures availability.

Answer: B Reference: CH01, What Is Information Security?

Explanation: Cryptography preserves confidentiality. Only those with the secret key can read an encoded note.

Type: Multiple Choice Difficulty: Medium Category: Understand

3. What is the practice of deliberately taking no action against an identified risk?

A. Risk mitigation
B. Risk transfer
C. Risk acceptance
D. Risk avoidance

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

Answer: C Reference: CH01, Risks

Explanation: An organization can decide to deliberately take no action against an identified risk, which is called risk acceptance. This type of strategy means that avoiding, mitigating, or transferring risk is not part of the organization's risk response plan.

Type: Multiple Choice Difficulty: Medium Category: Remember

4. What refers to applying safeguards to vulnerabilities and threats to lower risk to an acceptable level?

A. Residual risk
B. Risk avoidance
C. Risk mitigation
D. Risk transfer

Answer: C Reference: CH01, Risks

Explanation: Organizations can mitigate risk to reduce, but not eliminate, a negative impact. This response strategy is called risk mitigation. Using this strategy, organizations apply safeguards to vulnerabilities and threats to lower risk to an acceptable level.

Type: Multiple Choice Difficulty: Medium Category: Remember

5._____ means that only people with the right permission can access and use information.

A. Availability
B. Confidentiality
C. Integrity
D. Encryption

Answer: B Reference: CH01, What Is Confidentiality?

Explanation: Confidentiality means that only people with the right permission can access and use information.

Type: Multiple Choice Difficulty: Easy Category: Understand

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

6. Susan is a security professional. She has assessed her organization's IT environment for risks and determined that some risks are too expensive to be reduced. She decides to recommend the purchase of cyber liability insurance. Which of the following strategies is Susan practicing?

A. Risk mitigation
B. Risk transfer
C. Risk acceptance
D. Risk avoidance

Answer: B Reference: CH01, Risks

Explanation: In a strategy of risk transfer, an organization passes its risk to another entity, at which point the risk impact is borne by the other entity. An organization might choose this type of strategy when the cost of mitigating risk is more expensive than transferring it.

Type: Multiple Choice Difficulty: Medium Category: Apply

7. What involves tricking other people into breaking security procedures and sharing sensitive information?

A. Shoulder surfing
B. Logic bomb
C. Social engineering
D. Backdoor

Answer: C Reference: CH01, Social Engineering

Explanation: Social engineering is a type of attack that represents an intentional threat to confidentiality and relies heavily on human interaction.

Type: Multiple Choice Difficulty: Medium Category: Remember

8. What is the window of vulnerability?

A. The time between a malware attack and when antivirus software must be updated
B. The time between locating a target and launching a denial of service (DoS) attack
C. The time between a malware attack and discovery by security personnel
D. The time between exploit discovery and an installed security patch

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

Answer: D Reference: CH01, Vulnerabilities

Explanation: The window of vulnerability opens when someone discovers a vulnerability and closes when a vendor reduces or eliminates it. Exploits take place while the window is open.

Type: Multiple Choice Difficulty: Medium Category: Analyze

9. A single point of failure is a piece of hardware or application that is key to:

A. specifying how long systems may be offline before an organization starts to lose money.
B. the success of safeguards.
C. ensuring that individuals with proper permission can use systems and retrieve data in a dependable manner.
D. the functioning of the entire system.

Answer: D Reference: CH01, What Is Availability?

Explanation: A single point of failure is a piece of hardware or application that is key to the functioning of the entire system. If that single item fails, a critical portion of the system could fail. Single points of failure also can cause the whole system to fail.

Type: Multiple Choice Difficulty: Medium Category: Understand

10. Which of following is NOT one of the broad categories of vulnerabilities?

A. People
B. Process
C. Technology
D. Exploit

Answer: D Reference: CH01, Vulnerabilities

Explanation: A vulnerability is a weakness or flaw in an information system. The fourth broad category of vulnerabilities is Facility.

Type: Multiple Choice Difficulty: Medium Category: Remember

11. The separation of duties principle requires which of the following practices?

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

A. That two or more employees must split critical task functions so that no employee knows all of the steps of the critical task
B. That only one employee exclusively holds the knowledge about a critical function in an organization
C. That no two systems in an organization may provide similar services
D. That vendors provide hardware and software patches in a timely manner

Answer: A Reference: CH01, Vulnerabilities

Explanation: The separation of duties principle requires that two or more employees must split critical task functions so that no one employee knows all of the steps of the critical task. When only one employee knows all of the steps of a critical task, that employee can use the information to harm the organization.

Type: Multiple Choice Difficulty: Hard Category: Understand

12. Which of the following statements summarizes why the window of vulnerability is shrinking?

A. People are getting better at enduring exploits.
B. There are fewer people with the skills needed to create vulnerabilities.
C. More people are interested in information security and have developed the skills to find new vulnerabilities.
D. People are less inclined to attack vulnerabilities for financial gain.

Answer: C Reference: CH01, Vulnerabilities

Explanation: When people have skills to find new vulnerabilities, it then motivates them to make reports to the company that provides the product or service so the company can fix the vulnerability.

Type: Multiple Choice Difficulty: Medium Category: Understand

13. Which of the following is NOT true of phishing?

A. It is a form of internet fraud that takes place in electronic communications where attackers attempt to steal valuable information from their victims.
B. Spear phishing is a type of phishing scam in which attackers specifically target corporate executives.

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

C. A phishing message may request that recipients click on a uniform resource locator (URL) to verify their account details.
D. A phishing attack can take place via email, instant message, or an internet chat room.

Answer: B Reference: CH01, Phishing and Targeted Phishing Scams

Explanation: Whaling is a type of phishing scam in which attackers specifically target corporate executives. Spear phishing is a phishing scam in which attackers may target a particular organization.

Type: Multiple Choice Difficulty: Easy Category: Analyze

14. Which of the following is a method of controlled entry into a facility that uses two sets of doors, only one of which can be open at one time?

A. Fence
B. Mantrap
C. Least privilege
D. Security guard station

Answer: B Reference: CH01, Safeguards

Explanation: A mantrap is a method of controlled entry into a facility that provides access to secure areas. This method of entry has two sets of doors on either end of a small room. When a person enters a mantrap through one set of doors, the first set must close before the second set can open. This process effectively "traps" a person in the small room.

Type: Multiple Choice Difficulty: Easy Category: Understand

15. Which of the following is a type of safeguard that identifies a security incident while it is in progress?

A. Preventative
B. Detective
C. Corrective
D. Anomaly

Answer: B Reference: CH01, Safeguards

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

Explanation: Detective controls are safeguards put in place in order to detect, and sometimes report, a security incident while it is in progress. Examples of detective controls include logging system activity and reviewing the logs.

Type: Multiple Choice Difficulty: Medium Category: Understand

16. Whereas a(n) _____ is anything that can harm an information system, an exploit is a successful attack against a _____.

A. safeguard, vulnerability
B. risk, threat
C. threat, vulnerability
D. impact, risk

Answer: C Reference: CH01, Threats; Vulnerabilities

Explanation: A threat is anything that can harm an information system; an exploit is a successful attack against a vulnerability.

Type: Multiple Choice Difficulty: Hard Category: Analyze

17. What is the ISO/IEC 27002?

A. A reference guide to help organizations choose safeguards
B. A reference guide for standardized computing practices for large organizations
C. A reference guide to help organizations identify threats
D. A reference guide of common vulnerabilities in large organizations by type

Answer: A Reference: CH01, Choosing Safeguards

Explanation: ISO/IEC 27002 is a reference guide to help organizations choose safeguards.

Type: Multiple Choice Difficulty: Medium Category: Remember

18. What is the purpose of Executive Order 13526?

A. It grants the U.S. National Security Agency the right to wiretap suspected terrorists.
B. It provides a reference for helping companies choose safeguards.
C. It protects some types of consumer financial information.

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

D. It describes rules for using and a system for classifying national security information.

Answer: D Reference: CH01, U.S. National Security Information

Explanation: Executive Order 13526 describes rules for using and a system for classifying national security information.

Type: Multiple Choice Difficulty: Easy Category: Understand

19. Arturo is a security professional. He is strengthening the security of an information system. His design ensures that if a field should contain a number, the system checks the values that a user enters to make sure that the user actually entered numbers. The design also ensures that only authorized users have the ability to move or delete files. What is Arturo attempting to protect?

A. Confidentiality
B. Integrity
C. Availability
D. Vulnerabilities

Answer: B Reference: CH01, What Is Integrity?

Explanation: The described system design would protect data and information integrity.

Type: Multiple Choice Difficulty: Medium Category: Apply

20. Alice is a security professional. While scanning systems, she encounters malicious code that was set to carry out its functions when a specific event occurred in the future. What did Alice detect?

A. Keystroke logger
B. Backdoor
C. Logic bomb
D. Phishing email

Answer: C Reference: CH01, Logic Bombs

Explanation: A logic bomb is harmful code intentionally left on a computer system that lies dormant for a certain period. Programmers create logic bombs that explode on a certain day or

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

when a specific event occurs. Attackers also program logic bombs to explode in response to no action; for example, a logic bomb may explode when its creator does not log onto the target computer system for a predetermined number of days.

Type: Multiple Choice Difficulty: Medium Category: Apply

True/False Questions

1. Biometric data is considered personally identifiable information.

A. True
B. False

Answer: A Reference: CH01, Why Is Information Security an Issue?

Explanation: n/a

Type: True/False

2. An impact is the likelihood that a threat will exploit a vulnerability and cause harm.

A. True
B. False

Answer: B Reference: CH01, Risks

Explanation: A risk, not an impact, is the likelihood that a threat will exploit a vulnerability and cause harm.

Type: True/False

3. Organizations have a number of options for responding to risk, which include risk acceptance, risk avoidance, risk mitigation, and risk transfer.

A. True
B. False

Answer: A Reference: CH01, Risks

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

Explanation: n/a

Type: True/False

4. Integrity means that information systems and their data are accurate.

A. True
B. False

Answer: A Reference: CH01, What Is Integrity?

Explanation: n/a

Type: True/False

5. A vulnerability is anything that can cause harm to an information system.

A. True
B. False

Answer: B Reference: CH01, Risks

Explanation: A vulnerability is a weakness or flaw in an information system, whereas a risk is anything that can cause harm to an information system.

Type: True/False

6. Risk avoidance is the process of applying safeguards to avoid a negative impact.

A. True
B. False

Answer: A Reference: CH01, Risks

Explanation: n/a

Type: True/False

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

7. The workplace rule of "need to know" is an example of an administrative safeguard.

A. True
B. False

Answer: A Reference: CH01, Safeguards

Explanation: n/a

Type: True/False

8. Physical safeguards are actions that an organization takes to protect its tangible resources.

A. True
B. False

Answer: A Reference: CH01, Safeguards

Explanation: n/a

Type: True/False

9. Social engineering is any technology that secretly gathers information about a person or organization.

A. True
B. False

Answer: B Reference: CH01, Spyware and Keystroke Loggers

Explanation: Spyware is any technology that secretly gathers information about a person or organization.

Type: True/False

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

10. The U.S. security Secret data classification describes information that could cause damage to U.S. security if disclosed to an unauthorized person. This is the lowest data classification level.

A. True
B. False

Answer: B Reference: CH01, U.S. National Security Information

Explanation: The Confidential classification describes information that could cause damage to U.S. security if disclosed to an unauthorized person. It is the lowest data classification level. The Secret classification describes information that could cause serious damage if disclosed to an unauthorized person.

Type: True/False

11. A contract is a legal agreement between two or more parties that sets the ground rules for their relationship.

A. True
B. False

Answer: A Reference: CH01, Contracts

Explanation: n/a

Type: True/False

12. The United States has one comprehensive data protection law and relies on the Federal Trade Commission (FTC) to ensure compliance.

A. True
B. False

Answer: B Reference: CH01, Do Special Kinds of Data Require Special Kinds of Protection?

Explanation: The United States doesn't have one comprehensive data protection law. Several federal laws and agencies regulate compliance, including the Health Insurance Portability and

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

Accountability Act (HIPAA), the Department of Health and Human Services (HHS), and the Federal Trade Commission (FTC).

Type: True/False

13. Physical safeguards are the rules that state how systems will operate and are applied in the hardware and software of information systems.

A. True
B. False

Answer: B Reference: CH01, Safeguards

Explanation: Technical safeguards, also called logical safeguards, are applied in the hardware and software of information systems. Physical safeguards are actions that an organization takes to protect its actual, tangible resources.

Type: True/False

14. The C-I-A triad refers to the way that the Central Intelligence Agency classifies sensitive information.

A. True
B. False

Answer: B Reference: CH01, What Is Information Security?

Explanation: The C-I-A triad stands for the main information security goal of protecting the confidentiality, integrity, and availability of information.

Type: True/False

15. A personal identification number (PIN) is an example of an access control.

A. True
B. False

Answer: A Reference: CH01, What Is Confidentiality?

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

Explanation: n/a

Type: True/False

16. Patches exacerbate vulnerabilities because they mask problems.

A. True
B. False

Answer: B Reference: CH01, Vulnerabilities

Explanation: Patches update programs to address security or other operational problems.

Type: True/False

17. A high-quality security system can identify all threats, risks, and vulnerabilities.

A. True
B. False

Answer: B Reference: CH01, Threats

Explanation: It is not possible to identify every security vulnerability, to plan for every threat, or to identify all risks. Even when you identify risks, you cannot limit all risk of harm.

Type: True/False

18. There is no risk in clicking an email link as long as you do not enter personal information in the resulting web page.

A. True
B. False

Answer: B Reference: CH01, Phishing and Targeted Phishing Scams

Explanation: You can unintentionally download malware onto a computer when you click on a malicious link in an email.

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

Type: True/False

19. Organizations cannot control natural threats, such as earthquakes and tornadoes.

A. True
B. False

Answer: A Reference: CH01, Threats

Explanation: n/a

Type: True/False

20. Risk analysis is the process of reviewing known vulnerabilities and threats.

A. True
B. False

Answer: A Reference: CH01, Risks

Explanation: n/a

Type: True/False

Test Bank Statistics Summary

Multiple Choice
Category Stats
Analyze: 3
Apply: 3
Evaluate: 0
Remember: 5
Understand: 9

Difficulty Stats
Easy: 4 Medium: 14 Hard: 2

Total Multiple-Choice Questions: 20

Year revised: 2020

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama

True/False
Total True/False Questions: 20

Total Questions in Test Bank: 40

Access Complete Test Bank for Legal and Privacy Issues in Information Security 3rd Grama