

Pop Quiz 2 & 3

True/False

Indicate whether the statement is true or false.

1. An accurate inventory is important when performing a risk assessment. True or False?
2. Hardcopy printouts are not important if electronic copies are available.
3. A certain amount of risk is considered acceptable. True or False?
4. A projected risk must be based on the past experience of another company. True or False?
5. Risk refers to a company's ability to protect itself from the likelihood of an event occurring. True or False?

Multiple Choice

Identify the choice that best completes the statement or answers the question.

6. Which of the following are considered data/information?
 - a. Terminals
 - b. Operating Systems
 - c. Company Records
 - d. Commercial Software Products
7. Database management software fits into which of the following categories?
 - a. Data/Information
 - b. Software
 - c. Hardware
 - d. All of the Above
8. Databases fit into which of the following categories?
 - a. Data/Information
 - b. Software
 - c. Hardware
 - d. All of the Above
9. Why should you rank safeguards?
 - a. Management will never approve the safeguard with the highest cost.
 - b. It is not always practical to implement all solutions.
 - c. You may have to use a phased approach.
 - d. Ranking can keep you organized.
10. Safeguards might have to be eliminated from consideration for which of the following reasons?
 - a. Physical limitations
 - b. Financial limitations
 - c. Technical limitations
 - d. All of the Above
11. Alternatives to safeguards are important because of _____?
 - a. Availability of Resources
 - b. Acceptable Level of Risk
 - c. Different Levels of Protection
 - d. All of the Above
12. A company puts _____ in place to protect against an attack.
 - a. Risk
 - b. Safeguard
 - c. Vulnerability
 - d. Threat

Name: _____

ID: A

13. A _____ is considered a breakdown in company protection.
 - a. Risk
 - b. Safeguard
 - c. Vulnerability
 - d. Threat
14. An event that may disrupt noncritical business operations and cause employee inconvenience would be _____.
 - a. Issue
 - b. Serious
 - c. Severe
 - d. Catastrophic
15. An event that is classified as having significant history is considered to have a _____ likelihood of occurring.
 - a. Low
 - b. Medium
 - c. High
 - d. None of the Above
16. An event that may disrupt normal business operations would be classified as
 - a. Issue
 - b. Serious
 - c. Severe
 - d. Catastrophic
17. An event that is classified as having no history is considered to have a _____ likelihood of occurring.
 - a. Low
 - b. Medium
 - c. High
 - d. Critical
18. Which of the following is considered a safeguard?
 - a. After-Hours Security
 - b. Surveillance Cameras
 - c. Firewalls
 - d. All of the Above
19. Which level of potential risk requires attention and safeguard implementation in the near future?
 - a. High
 - b. Moderate
 - c. Low
 - d. None of the Above

Completion

Complete each statement.

20. One of the looming fears is the increasing number of _____ attacks.
21. One of the primary defenses against attacks is applying _____, software that repairs security flaws and other problems in an application or operating system.
22. _____ ensures that only authorized parties can view information.
23. _____ is often associated with theft prevention.
24. One of the most important objectives of information security is to protect important _____ and _____ data from theft.
25. The _____ requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information.

Name: _____

ID: A

- 26. One challenge in combating _____ is that many prime targets are not owned and managed by the federal government.
- 27. A(n) _____ is a person or thing that has the power to carry out a threat.
- 28. A(n) _____ is the likelihood that something will happen.
- 29. _____ help employers determine who has the skills and knowledge necessary to secure their systems and data.

Short Answer

- 30. Which are potential consequences of an event that occurs as a result of a breach?

Pop Quiz 2 & 3 Answer Section

TRUE/FALSE

- | | |
|-----------|--------|
| 1. ANS: T | PTS: 1 |
| 2. ANS: F | PTS: 1 |
| 3. ANS: T | PTS: 1 |
| 4. ANS: F | PTS: 1 |
| 5. ANS: T | PTS: 1 |

MULTIPLE CHOICE

- | | |
|------------|--------|
| 6. ANS: C | PTS: 1 |
| 7. ANS: B | PTS: 1 |
| 8. ANS: A | PTS: 1 |
| 9. ANS: B | PTS: 1 |
| 10. ANS: D | PTS: 1 |
| 11. ANS: D | PTS: 1 |
| 12. ANS: B | PTS: 1 |
| 13. ANS: C | PTS: 1 |
| 14. ANS: A | PTS: 1 |
| 15. ANS: C | PTS: 1 |
| 16. ANS: B | PTS: 1 |
| 17. ANS: A | PTS: 1 |
| 18. ANS: D | PTS: 1 |
| 19. ANS: B | PTS: 1 |

COMPLETION

- | | |
|--------------------------------|--|
| 20. ANS: Zero-day | |
| PTS: 1 | |
| 21. ANS: Patches | |
| PTS: 1 | |
| 22. ANS: Integrity | |
| PTS: 1 | |
| 23. ANS: Security | |
| PTS: 1 | |
| 24. ANS: Business and Personal | |
| PTS: 2 | |

25. ANS: Gramm-Leach-Bliley Act or GLBA

PTS: 1

26. ANS: Cybercrime / Cyberterrorism

PTS: 1

27. ANS: Threat agent / Malicious actor

PTS: 1

28. ANS: Risk

PTS: 1

29. ANS: Certifications

PTS: 1

SHORT ANSWER

30. ANS:
Loss of assets, privacy, trust, service

PTS: 1