

Mod 1 Introduction to Information Security

True / False

1. During the early years of computing, the primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage.

- a. True
- b. False

ANSWER: True

2. Network security focuses on the protection of physical items, objects, or areas from unauthorized access and misuse.

- a. True
- b. False

ANSWER: False

3. When a computer is the subject of an attack, it is the entity being attacked.

- a. True
- b. False

ANSWER: False

4. The value of information comes from the characteristics it possesses.

- a. True
- b. False

ANSWER: True

5. E-mail spoofing involves sending an e-mail message with a harmful attachment.

- a. True
- b. False

ANSWER: False

6. The possession of information is the quality or state of having value for some purpose or end.

- a. True
- b. False

ANSWER: False

7. A breach of possession may not always result in a breach of confidentiality.

- a. True
- b. False

ANSWER: True

8. Hardware is often the most valuable asset possessed by an organization, and it is the main target of intentional attacks.

- a. True
- b. False

ANSWER: False

9. Information security can be an absolute.

Mod 1 Introduction to Information Security

- a. True
- b. False

ANSWER: False

10. To achieve balance—that is, to operate an information system that satisfies the user and the security professional—the security level must allow reasonable access, yet protect against threats.

- a. True
- b. False

ANSWER: True

11. The bottom-up approach to information security has a higher probability of success than the top-down approach.

- a. True
- b. False

ANSWER: False

12. Using a methodology will usually have no effect on the probability of success.

- a. True
- b. False

ANSWER: False

13. A champion is a project manager, who may be a departmental line manager or staff unit manager, and has expertise in project management and information security technical requirements.

- a. True
- b. False

ANSWER: False

14. A data custodian works directly with data owners and is responsible for the storage, maintenance, and protection of the information.

- a. True
- b. False

ANSWER: True

15. The roles of information security professionals focus on protecting the organization's information systems and stored information from attacks.

- a. True
- b. False

ANSWER: True

Modified True / False

16. Every organization, whether public or private and regardless of size, has information it wants to protect. _____

ANSWER: True

17. The history of information security begins with the concept of communications security. _____

ANSWER: False - computer

Mod 1 Introduction to Information Security

18. RAND Report R-609 was the first widely recognized published document to identify the role of management and policy issues in computer security. _____

ANSWER: True

19. Much of the early research on computer security centered on a system called Management Information and Computing Service (MULTICS). _____

ANSWER: False - Multiplexed

20. According to the CNSS, networking is “the protection of information and its critical elements.” _____

ANSWER: False - information security

21. Indirect attacks originate from a compromised system or resource that is malfunctioning or working under the control of a threat. _____

ANSWER: True

22. When unauthorized individuals or systems can view information, confidentiality is breached. _____

ANSWER: True

23. Confidentiality ensures that only those with the rights and privileges to access information are able to do so. _____

ANSWER: True

24. Information has redundancy when it is free from mistakes or errors and it has the value that the end user expects. _____

ANSWER: False - accuracy

25. Hardware is the physical technology that houses and executes the software, stores and transports the data, and provides interfaces for the entry and removal of information from the system. _____

ANSWER: True

26. A(n) hardware system is the entire set of people, procedures, and technology that enable business to use information. _____

ANSWER: False - information

27. Information security can begin as a grassroots effort in which systems administrators attempt to improve the security of their systems, often referred to as the bottom-up approach. _____

ANSWER: True

28. The role of the project manager—typically an executive such as a chief information officer (CIO) or the vice president of information technology (VP-IT)—in this effort cannot be overstated. _____

ANSWER: False - champion

29. Of the two approaches to information security implementation, the top-down approach has a higher probability of success. _____

ANSWER: True

30. A(n) project team should consist of a number of individuals who are experienced in one or multiple facets of the

Mod 1 Introduction to Information Security

technical and nontechnical areas. _____

ANSWER: True

Multiple Choice

31. _____ is a network project that preceded the Internet.

- | | |
|---------|------------|
| a. NIST | b. ARPANET |
| c. FIPS | d. DES |

ANSWER: b

32. Which of the following was not an identified fundamental problem with ARPANET security?

- a. phone numbers for access were closely held and distributed on a need-to-know basis
- b. vulnerability of password structure and formats
- c. lack of safety procedures for dial-up connections
- d. nonexistent user identification and authorizations

ANSWER: a

33. The famous study entitled "Protection Analysis: Final Report" focused on a project undertaken by ARPA to understand and detect _____ in operating systems security.

- | | |
|------------|----------------------|
| a. bugs | b. vulnerabilities |
| c. malware | d. maintenance hooks |

ANSWER: b

34. _____ was the first operating system to integrate security as one of its core functions.

- | | |
|------------|------------|
| a. UNIX | b. DOS |
| c. MULTICS | d. ARPANET |

ANSWER: c

35. In 1993, the first _____ conference was held in Las Vegas. Originally, it was established as a gathering for people interested in information security, including authors, lawyers, government employees, and law enforcement officials.

- a. DEFCON
- b. CyberCom
- c. Black Hat
- d. World Security

ANSWER: a

36. The protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology is known as _____.

- a. communications security
- b. network security
- c. physical security
- d. information security

Mod 1 Introduction to Information Security

ANSWER:

d

37. A server would experience a(n) _____ attack when a hacker compromises it to acquire information via a remote location using a network connection.

- | | | | |
|----|----------|----|----------|
| a. | indirect | b. | direct |
| c. | software | d. | hardware |

ANSWER:

b

38. A subject or object's ability to use, manipulate, modify, or affect another subject or object is known as _____.

- | | |
|----|----------|
| a. | access |
| b. | assets |
| c. | exploits |
| d. | risk |

ANSWER:

a

39. An organizational resource that is being protected is sometimes logical, such as a Web site, software information, or data. Sometimes the resource is physical, such as a person, computer system, hardware, or other tangible object. Either way, the resource is known as a(n) _____.

- | | |
|----|---------------|
| a. | access method |
| b. | asset |
| c. | exploit |
| d. | risk |

ANSWER:

b

40. A computer is the _____ of an attack when it is used to conduct an attack against another computer.

- | | | | |
|----|---------|----|-------------|
| a. | subject | b. | object |
| c. | target | d. | facilitator |

ANSWER:

a

41. A technique used to compromise a system is known as a(n) _____.

- | | |
|----|---------------|
| a. | access method |
| b. | asset |
| c. | exploit |
| d. | risk |

ANSWER:

c

42. In file hashing, a file is read by a special algorithm that uses the value of the bits in the file to compute a single number called the _____ value.

- | | | | |
|----|--------|----|----------|
| a. | result | b. | smashing |
| c. | hash | d. | code |

ANSWER:

c

43. _____ of information is the quality or state of being genuine or original.

- | | | | |
|----|--------------|----|----------|
| a. | Authenticity | b. | Spoofing |
|----|--------------|----|----------|

Mod 1 Introduction to Information Security

c. Confidentiality

d. Authorization

ANSWER:

a

44. _____ has become a widely accepted evaluation standard for training and education related to the security of information systems and is hosted by CNSS.

a. NIST SP 800-12

b. NSTISSI No. 4011

c. IEEE 802.11(g)

d. ISO 17788

ANSWER:

b

45. _____ security addresses the issues necessary to protect the tangible items, objects, or areas of an organization from unauthorized access and misuse.

a. Physical

b. Personal

c. Object

d. Standard

ANSWER:

a

46. An information system is the entire set of _____, people, procedures, and networks that enable the use of information resources in the organization.

a. software

b. hardware

c. data

d. All of the above

ANSWER:

d

47. The protection of tangible items, objects, or areas from unauthorized access and misuse is known as _____.

a. communications security

b. network security

c. physical security

d. information security

ANSWER:

c

48. The _____ is the individual primarily responsible for the assessment, management, and implementation of information security in the organization.

a. ISO

b. CIO

c. CISO

d. CTO

ANSWER:

c

49. Which of the following is a valid type of role when it comes to data ownership?

a. Data owners

b. Data custodians

c. Data users

d. All of the above

ANSWER:

d

50. People with the primary responsibility for administering the systems that house the information used by the organization perform the role of _____.

a. Security policy developers

b. Security professionals

c. System administrators

Mod 1 Introduction to Information Security

- d. End users

ANSWER:

c

51. Individuals who control, and are therefore ultimately responsible for, the security and use of a particular set of information are known as data _____.

- a. owners
- b. custodians
- c. trustees
- d. users

ANSWER:

a

52. Individuals who are assigned the task of managing a particular set of information and coordinating its protection, storage, and use are known as data _____.

- a. owners
- b. custodians
- c. trustees
- d. users

ANSWER:

c

53. The community of interest made up of IT managers and skilled professionals in systems design, programming, networks, and other related disciplines is called _____.

- a. Information Technology Management and Professionals
- b. Organizational Management and Professionals
- c. Information Security Management and Professionals
- d. Executive Management

ANSWER:

a

Completion

54. The history of information security begins with the concept of _____ security.

ANSWER:

computer

55. During the early years, information security was a straightforward process composed predominantly of _____ security and simple document classification schemes.

ANSWER:

physical

56. During the _____ War, many mainframes were brought online to accomplish more complex and sophisticated tasks, so it became necessary to enable the mainframes to communicate via a less cumbersome process than mailing magnetic tapes between computer centers.

ANSWER:

Cold

57. The Internet brought _____ to virtually all computers that could reach a phone line or an Internet-connected local area network.

ANSWER:

connectivity

Mod 1 Introduction to Information Security

58. The CNSS model of information security evolved from a concept developed by the computer security industry known as the _____ triad.

ANSWER: CIA
C.I.A.
Confidentiality, Integrity, and Availability

59. A computer is the _____ of an attack when it is the entity being targeted.

ANSWER: object

60. The probability of an unwanted occurrence, such as an adverse event or loss, is known as a(n) _____.

ANSWER: risk

61. Any event or circumstance that has the potential to adversely affect operations and assets is known as a(n) _____.

ANSWER: threat

62. In an organization, the value of _____ of information is especially high when it involves personal information about employees, customers, or patients.

ANSWER: confidentiality

63. A potential weakness in an asset or its defensive control system(s) is known as a(n) _____.

ANSWER: vulnerability

64. Information has _____ when it is whole, complete, and uncorrupted.

ANSWER: integrity

65. _____ enables authorized users—people or computer systems—to access information without interference or obstruction and to receive it in the required format.

ANSWER: Availability

66. _____ of information is the quality or state of being genuine or original, rather than a reproduction or fabrication.

ANSWER: Authenticity

67. The _____ of information is the quality or state of ownership or control of some object or item.

ANSWER: possession

68. The _____ component of an information system comprises applications, operating systems, and assorted command utilities.

ANSWER: software

69. Software is often created under the constraints of _____ management, placing limits on time, cost, and manpower.

ANSWER: project

70. A frequently overlooked component of an information system, _____ are the written instructions for accomplishing a specific task.

ANSWER: procedures

71. The senior technology officer is typically the chief _____ officer.

Mod 1 Introduction to Information Security

ANSWER: information

72. A(n) _____ is a group of individuals who are united by similar interests or values within an organization and who share a common goal of helping the organization to meet its objectives.

ANSWER: community of interest

Essay

73. Describe the multiple types of security systems present in many organizations.

ANSWER: A successful organization should have multiple layers of security in place to protect its operations, including physical, networks, and information:

Physical security, to protect physical items, objects, or areas from unauthorized access and misuse

Network security, to protect networking components, connections, and contents

Information security, to protect the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

74. Outline types of data ownership and their respective responsibilities.

ANSWER: Data owners: Those responsible for the security and use of a particular set of information. They are usually members of senior management and could be CIOs. The data owners usually determine the level of data classification associated with the data, as well as the changes to that classification required by organizational change.

Data custodians: Working directly with data owners, data custodians are responsible for the storage, maintenance, and protection of the information. The duties of a data custodian often include overseeing data storage and backups, implementing the specific procedures and policies laid out in the security policies and plans, and reporting to the data owner.

Data users: End users who work with the information to perform their daily jobs supporting the mission of the organization. Data users are included as individuals with an information security role.

Subjective Short Answer

75. What is the difference between a threat agent and a threat source?

ANSWER: A threat agent is the facilitator of an attack, whereas a threat source is a category of objects, people, or other entities that represents a potential danger to an asset. Threats are always present. Some threats manifest themselves in accidental occurrences and others are purposeful. Fire is a threat; however, a fire that has begun in a building is an attack. If an arsonist set the fire, then the arsonist is the threat agent. If an accidental electrical short started the fire, the short is the threat agent.

76. Describe the need for balance between information security and access to information inherent in information systems.

ANSWER: To achieve balance—that is, to operate an information system that satisfies the user and the security professional—the security level must allow reasonable access yet protect against threats.

77. Should the overall approach to security be more managerial or technical?

Name _____ Class _____ Date _____
: _____ : _____ e: _____

Mod 1 Introduction to Information Security

ANSWER: The approach to security should be more managerial than technical, although the technical ability of the resources who perform day-to-day activities is critical. The top-down approach to security implementation is by far the best. It has strong upper management support, a dedicated champion, dedicated funding, clear planning, and the opportunity to influence organizational culture.

78. Describe the role of a data trustee.

ANSWER: Data trustees are individuals appointed by data owners to oversee the management of a particular set of information and to coordinate with data custodians for its storage, protection, and use. Because data owners are typically top-level executives and managers too busy to oversee the management of their data, they will typically appoint a senior subordinate as a data trustee to handle those responsibilities.