Name: _____ Class: _____ Date: _____

Chapter 01: 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. The value of information comes from the characteristics it possesses.

a. True
b. False

ANSWER: True

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

a. True
b. False

ANSWER: False

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.

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. The implementation phase is the longest and most expensive phase of the systems development life cycle (SDLC).

a. True
b. False

ANSWER: False

14. The investigation phase of the SDLC involves specification of the objectives, constraints, and scope of the project.

a. True
b. False

ANSWER: True

15. The physical design is the blueprint for the desired solution.

a. True
b. False

ANSWER: False

16. In the physical design phase, specific technologies are selected.

a. True
b. False

ANSWER: True

17. The water-ski model is a type of SDLC in which each phase of the process flows from the information gained in the previous phase, with multiple opportunities to return to previous phases and make adjustments.

a. True

b. False

ANSWER: False

18. 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

19. 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

20. The roles of information security professionals are almost always aligned with the goals and mission of the information security community of interest.

a. True
b. False

ANSWER: True

Modified True / False

21. MULTICS stands for Multiple Information and Computing Service. _____

ANSWER: False - Multiplexed

22. According to the CNSS, networking is "the protection of information and its critical elements."

_____

ANSWER: False - information security

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

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

_____

ANSWER: True

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

_____

ANSWER: True

Chapter 01: Introduction to Information Security

27. 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

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

29. 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

30. Key end users should be assigned to a developmental team, known as the united application development team. _____
ANSWER: False - joint

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

32. The Security Development Life Cycle (SDLC) is a general methodology for the design and implementation of an information system. _____
ANSWER: False - Systems

33. The Analysis phase of the SDLC examines the event or plan that initiates the process and specifies the objectives, constraints, and scope of the project. _____
ANSWER: False - Investigation

34. SecOps focuses on integrating the need for the development team to provide iterative and rapid improvements to system functionality and the need for the operations team to improve security and minimize the disruption from software release cycles. _____
ANSWER: False - DevOps

35. A(n) project team should consist of a number of individuals who are experienced in one or multiple facets of the technical and nontechnical areas. _____
ANSWER: True

Multiple Choice

36. _____ is a network project that preceded the Internet.
a. NIST b. ARPANET
c. FIPS d. DES
ANSWER: b

37. 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

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

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

ANSWER: c

39. _____ 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

40. 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

41. 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

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

a. Authenticity b. Spoofing
c. Confidentiality d. Authorization

ANSWER: a

43. 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

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

a. NIST SP 800-12 b. NSTISSI No. 4011
c. IEEE 802.11(g) d. ISO 17788

ANSWER: b

45. 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

46. A methodology and formal development strategy for the design and implementation of an information system is referred to as a _____.

a. systems design
b. development life project
c. systems development life cycle
d. systems schema

ANSWER: c

47. An emerging methodology to integrate the effort of the development team and the operations team to improve the functionality and security of applications is known as _____.

a. SDLC
b. DevOps
c. JAD/RAD
d. SecOps

ANSWER: b

48. A type of SDLC in which each phase has results that flow into the next phase is called the _____ model.

a. pitfall
b. SA&D
c. waterfall
d. Method 7

ANSWER: c

49. During the _____ phase, specific technologies are selected to support the alternatives identified and evaluated in the prior phases.

a. investigation
b. implementation
c. analysis
d. physical design

ANSWER: d

50. Which of the following phases is often considered the longest and most expensive phase of the systems development life cycle?

a. investigation
b. logical design
c. implementation
d. maintenance and change

ANSWER: d

51. Organizations are moving toward more _____-focused development approaches, seeking to improve not only the functionality of the systems they have in place, but consumer confidence in their product.

a. security
b. reliability
c. accessibility
d. availability

ANSWER: a

52. The _____ design phase of an SDLC methodology is implementation independent, meaning that it contains no reference to specific technologies, vendors, or products.

a. conceptual
b. logical
c. integral
d. physical

ANSWER: b

53. 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

54. 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

55. 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
d. End users

ANSWER: c

56. The protection of all communications media, technology, and content is known as _____.

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

ANSWER: a

57. 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

ANSWER: d

58. 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

59. 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

60. 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

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

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

ANSWER: c

Completion

62. The history of information security begins with the concept of _____ security.
ANSWER: computer

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

64. 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

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

66. 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

67. A computer is the _____ of an attack when it is the entity being targeted.
ANSWER: object

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

69. _____ of information is the quality or state of being genuine or original, rather than a reproduction or fabrication.
ANSWER: Authenticity

70. Information has _____ when it is whole, complete, and uncorrupted.
ANSWER: integrity

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

72. The _____ of information is the quality or state of ownership or control of some object or item.
ANSWER: possession

73. The _____ component of an information system comprises applications, operating systems, and assorted command utilities.
ANSWER: software

74. Software is often created under the constraints of _____ management, placing limits on time, cost, and manpower.
ANSWER: project

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

76. In the _____ approach, the project is initiated by upper-level managers who issue policy, procedures, and processes, dictate the goals and expected outcomes, and determine accountability for each required action.
ANSWER: top-down

77. A(n) _____ is a formal approach to solving a problem by means of a structured sequence of procedures.
ANSWER: methodology

78. The _____ phase consists primarily of assessments of the organization, its current systems, and its capability to support the proposed systems.
ANSWER: analysis

79. During the _____ phase of the systems life cycle, the process begins by examining the event or plan that initiated the process. During this phase, the objectives, constraints, and scope of the project are specified.

Chapter 01: Introduction to Information Security

ANSWER: investigation

80. The senior technology officer is typically the chief _____ officer.
ANSWER: information

81. 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

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

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

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

Essay

85. Describe the multiple types of security systems present in many organizations.
ANSWER: A successful organization should have the following multiple layers of security in place to protect its operations, including physical, personnel, operations, communications, networks, and information:

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

Personnel security, to protect the individual or group of individuals who are authorized to access the organization and its operations

Operations security, to protect the details of a particular operation or series of activities

Communications security, to protect communications media, technology, and content

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.

86. List and describe the phases of the traditional systems development life cycle.
ANSWER: Investigation
The investigation phase begins with a directive from upper management, dictating the process, outcomes, and goals of the project, as well as its budget and other constraints. Frequently, this phase begins with an **enterprise information security policy**, which outlines the implementation of a security program within the organization. Teams of responsible managers, employees, and contractors are organized; problems are analyzed; and the scope of the project, as well as specific goals and objectives, and any additional constraints not covered in the program policy, are defined. Finally, an organizational feasibility analysis is performed to determine whether the organization has the resources and commitment necessary to conduct a successful

security analysis and design.

Analysis
In the analysis phase, the documents from the investigation phase are studied. The development team conducts a preliminary analysis of existing security policies or programs, along with that of documented current threats and associated controls. This phase also includes an analysis of relevant legal issues that could affect the design of the security solution. Increasingly, privacy laws have become a major consideration when making decisions about information systems that manage personal information. Recently, many states have implemented legislation making certain computer-related activities illegal. A detailed understanding of these issues is vital. The risk management task also begins in this stage. **Risk management** is the process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the organization's security and to the information stored and processed by the organization.

Logical Design
The logical design phase creates and develops the blueprints for information security, and examines and implements key policies that influence later decisions. Also at this stage, the team plans the incident response actions to be taken in the event of partial or catastrophic loss. The planning answers the following questions:
- Continuity planning: How will business continue in the event of a loss?
- Incident response: What steps are taken when an attack occurs?
- Disaster recovery: What must be done to recover information and vital systems immediately after a disastrous event?

Next, a feasibility analysis determines whether the project should be continued or outsourced.

Physical Design
In the physical design phase, the information security technology needed to support the blueprint outlined in the logical design is evaluated, alternative solutions generated, and a final design agreed upon. The information security blueprint may be revisited to keep it in line with the changes needed when the physical design is completed. Criteria for determining the definition of successful solutions are also prepared during this phase. Included at this time are the designs for physical security measures to support the proposed technological solutions. At the end of this phase, a feasibility study should determine the readiness of the organization for the proposed project, and then the champion and sponsors are presented with the design. At this time, all parties involved have a chance to approve the project before implementation begins.

Implementation
In the implementation phase, the security solutions are acquired (made or bought), tested, implemented, and tested again. Personnel issues are evaluated, and specific training and education programs conducted. Finally, the entire tested package is presented to upper management for final approval.

Maintenance and Change
The maintenance and change phase, though last, is perhaps most important, given the current ever-changing threat environment. Today's information security systems need constant monitoring, testing, modification, updating, and repairing. Traditional applications systems developed within the framework of the traditional SDLC are not designed to anticipate a vicious attack that would require some degree of application reconstruction. In information security, the battle for stable, reliable systems is a defensive one. Often, repairing damage and restoring information is a constant effort against an unseen adversary. As new threats emerge and old threats evolve, the information security profile of an organization requires constant adaptation to prevent threats from successfully penetrating sensitive data. This constant vigilance and security can be compared to that of a fortress where threats from outside as well as from within must be constantly monitored and checked with continuously new and more innovative technologies.

Chapter 01: Introduction to Information Security

87. 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.