TRUE/FALSE

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

   ANS: T PTS: 1 REF: 3

2. Network security focuses on the protection of the details of a particular operation or series of activities.

   ANS: F PTS: 1 REF: 8

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

   ANS: T PTS: 1 REF: 11

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

   ANS: F PTS: 1 REF: 11

5. An e-mail virus involves sending an e-mail message with a modified field.

   ANS: F PTS: 1 REF: 12

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

   ANS: F PTS: 1 REF: 15

7. A breach of possession always results in a breach of confidentiality.

   ANS: F PTS: 1 REF: 15

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

   ANS: F PTS: 1 REF: 17

9. Information security can be an absolute.

   ANS: F PTS: 1 REF: 19

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.

    ANS: T PTS: 1 REF: 19

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

    ANS: F PTS: 1 REF: 20

12. Using a methodology increases the probability of success.

    ANS: T PTS: 1 REF: 21

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

    ANS: F PTS: 1 REF: 23

14. The investigation phase of the SecSDLC begins with a directive from upper management.

    ANS: T PTS: 1 REF: 26

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

    ANS: F PTS: 1 REF: 27

16. Recently, many states have implemented legislation making certain computer-related activities illegal.

    ANS: T PTS: 1 REF: 27

17. Applications systems developed within the framework of the traditional SDLC are designed to anticipate a software attack that requires some degree of application reconstruction.

    ANS: F PTS: 1 REF: 29

18. A champion is a project manager, who may be a departmental line manager or staff unit manager, and understands project management, personnel management, and information security technical requirements.

    ANS: F PTS: 1 REF: 30

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

    ANS: T PTS: 1 REF: 30

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

    ANS: T PTS: 1 REF: 31

MODIFIED TRUE/FALSE

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

   ANS: F, Multiplexed

   PTS: 1 REF: 6

2. In general, protection is "the quality or state of being secure—to be free from danger."
   _____

ANS: F, security

PTS: 1 REF: 8

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

ANS: F, Indirect

PTS: 1 REF: 9

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

ANS: F, accuracy

PTS: 1 REF: 12

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

ANS: T PTS: 1 REF: 13

6. In information security, salami theft occurs when an employee steals a few pieces of information at a time, knowing that taking more would be noticed — but eventually the employee gets something complete or useable. _____

ANS: T PTS: 1 REF: 13

7. 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. _____

ANS: T PTS: 1 REF: 17

8. Policies are written instructions for accomplishing a specific task. _____

ANS: F, Procedures

PTS: 1 REF: 18

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

ANS: T PTS: 1 REF: 20

10. Key end users should be assigned to a developmental team, known as the united application development team. _____

ANS: F, joint

PTS: 1 REF: 20

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

    ANS: T PTS: 1 REF: 20

12. The Security Development Life Cycle (SDLC) is a methodology for the design and implementation of an information system. _____

    ANS: F, Systems

    PTS: 1 REF: 21

13. The Analysis phase of the SecSDLC begins with a directive from upper management. _____

    ANS: F, Investigation

    PTS: 1 REF: 26

14. Risk evaluation 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. _____

    ANS: F, management

    PTS: 1 REF: 27

15. 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. _____

    ANS: T PTS: 1 REF: 30

MULTIPLE CHOICE

1. ____ is the predecessor to the Internet.
   a. NIST
   b. ARPANET
   c. FIPS
   d. DES

   ANS: B PTS: 1 REF: 4

2. A famous study entitled "Protection Analysis: Final Report" was published in ____.
   a. 1868
   b. 1978
   c. 1988
   d. 1998

   ANS: B PTS: 1 REF: 5

3. ____ was the first operating system to integrate security as its core functions.
   a. UNIX
   b. DOS
   c. MULTICS
   d. ARPANET

   ANS: C PTS: 1 REF: 6-7

4. ____ 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

ANS: A PTS: 1 REF: 8

5. A(n) ____ attack is a hacker using a personal computer to break into a system.
a. indirect
b. direct
c. software
d. hardware

ANS: B PTS: 1 REF: 9

6. A computer is the ____ of an attack when it is used to conduct the attack.
a. subject
b. object
c. target
d. facilitator

ANS: A PTS: 1 REF: 11

7. ____ of information is the quality or state of being genuine or original.
a. Authenticity
b. Spoofing
c. Confidentiality
d. Authorization

ANS: A PTS: 1 REF: 12

8. 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 large number called a ____ value.
a. key
b. hashing
c. hash
d. code

ANS: C PTS: 1 REF: 14

9. ____ presents a comprehensive information security model and has become a widely accepted evaluation standard for the security of information systems.
a. NIST SP 800-12
b. NSTISSI No. 4011
c. IEEE 802.11(g)
d. ISO 17788

ANS: B PTS: 1 REF: 15

10. An information system is the entire set of ____, people, procedures, and networks that make possible the use of information resources in the organization.
a. software
b. hardware
c. data
d. All of the above

ANS: D PTS: 1 REF: 16

11. The most successful kind of top-down approach involves a formal development strategy referred to as a ____.
a. systems design
b. development life project
c. systems development life cycle
d. systems schema

ANS: C PTS: 1 REF: 20

12. The ____ is a methodology for the design and implementation of an information system in an organization.
a. DSLC
b. SDLC
c. LCSD
d. CLSD

ANS: B PTS: 1 REF: 21

13. The ____ model consists of six general phases.
    a. pitfall
    b. 5SA&D
    c. waterfall
    d. SysSP

    ANS: C PTS: 1 REF: 21

14. During the ____ phase, specific technologies are selected to support the alternatives identified and evaluated in the logical design.
    a. investigation
    b. implementation
    c. analysis
    d. physical design

    ANS: D PTS: 1 REF: 23

15. Which of the following phases is the longest and most expensive phase of the systems development life cycle?
    a. investigation
    b. logical design
    c. implementation
    d. maintenance and change

    ANS: D PTS: 1 REF: 23

16. 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

    ANS: A PTS: 1 REF: 26

17. Part of the logical design phase of the SecSDLC is planning for partial or catastrophic loss. ____ dictates what steps are taken when an attack occurs.
    a. Continuity planning
    b. Incident response
    c. Disaster recovery
    d. Security response

    ANS: B PTS: 1 REF: 27

18. 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

    ANS: C PTS: 1 REF: 29

19. Which of the following is a valid type of data ownership?
    a. Data owners
    b. Data custodians
    c. Data users
    d. All of the above

    ANS: D PTS: 1 REF: 30

20. People with the primary responsibility for administering the systems that house the information used by the organization perform the ____ role.
    a. security policy developers
    b. security professionals
    c. system administrators
    d. end users

    ANS: C PTS: 1 REF: 30

COMPLETION

1. The history of information security begins with the history of _____ security.

   ANS: computer

   PTS: 1 REF: 3

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

   ANS: physical

   PTS: 1 REF: 3

3. 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.

   ANS: Cold

   PTS: 1 REF: 4

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

   ANS: network

   PTS: 1 REF: 7

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

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

   PTS: 1 REF: 8

6. A computer is the _____ of an attack when it is the target entity.

   ANS: object

   PTS: 1 REF: 11

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

   ANS: Availability

   PTS: 1 REF: 12

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

ANS: Authenticity

PTS: 1 REF: 12

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

ANS: integrity

PTS: 1 REF: 13

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

ANS: confidentiality

PTS: 1 REF: 13

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

ANS: possession

PTS: 1 REF: 15

12. The _____ component of the IS comprises applications, operating systems, and assorted command utilities.

ANS: software

PTS: 1 REF: 16

13. _____ carries the lifeblood of information through an organization.

ANS: Software

PTS: 1 REF: 16

14. A frequently overlooked component of an IS, _____ are written instructions for accomplishing a specific task.

ANS: procedures

PTS: 1 REF: 18

15. 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.

ANS: top-down

PTS: 1 REF: 20

16. A(n) _____ is a formal approach to solving a problem by means of a structured sequence of procedures.

    ANS: methodology

    PTS: 1 REF: 21

17. The _____ phase consists primarily of assessments of the organization, its current systems, and its capability to support the proposed systems.

    ANS: analysis

    PTS: 1 REF: 22

18. A(n) _____ information security policy outlines the implementation of a security program within the organization.

    ANS: enterprise

    PTS: 1 REF: 26

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

    ANS: information

    PTS: 1 REF: 29

20. 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.

    ANS: community of interest

    PTS: 1 REF: 31

ESSAY

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

   ANS:
   A successful organization should have the following multiple layers of security in place to protect its operations:

   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.

PTS: 1 REF: 8

2. List and describe the six phases of the security systems development life cycle.

ANS:
Investigation
The investigation phase of the SecSDLC 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 or not the project should be continued or be 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
The implementation phase in of SecSDLC is also similar to that of the traditional SDLC. 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.

PTS: 1 REF: 26-29

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

ANS:
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.

PTS: 1 REF: 30