Test Bank for Information Security Text and Cases 2nd Dhillon

Access Complete Test Bank for Information Security Text and Cases 2nd Dhillon

Multiple Choice Questions

Chapter 2—Security of Technical Systems in Organizations

1. When dealing with information system security, the weakest point is considered to be the most serious vulnerability. This is generally termed as the principle of _____.
    a. weakest node
    b. easiest penetration
    c. easiest threat
    d. weakest entry point
2. Perpetrators generally stick to the _____ means to accomplish their objectives.
    a. easiest and safest
    b. easiest and simplest
    c. safest and simplest
    d. easiest, safest, and simplest
3. Which of the following vulnerability applies to hardware, software, and data?
    a. Destruction
    b. Interception
    c. Modification
    d. Disclosure
4. Fabrication and disclosure vulnerabilities only apply to _____.
    a. hardware
    b. software
    c. data
    d. none of the above
5. _____ is said to occur when the data held in a computer system is accessed in an unauthorized manner and is changed without requisite permissions.
    a. Modification
    b. Destruction
    c. Disclosure
    d. Interception
6. _____ occurs simply when the hardware, software, or the data are destroyed because of malicious intent.
    a. Modification
    b. Destruction
    c. Disclosure
    d. Interception
7. _____ of data takes place when data are made available or access to software is made available without due consent of the individual responsible for the data or software.
    a. Modification
    b. Destruction
    c. Disclosure
    d. Interception
8. _____ occurs when an unauthorized person or software gains access to data or computer resources.
    a. Modification
    b. Destruction
    c. Disclosure
    d. Interception
9. _____ occurs when a computer system becomes unavailable for use.
    a. Disclosure
    b. Interception

Access Complete Test Bank for Information Security Text and Cases 2nd Dhillon

c. Interruption
d. Fabrication

10. _____ occurs when spurious transactions are inserted into a network or records are added to an existing database.
    a. Disclosure
    b. Interception
    c. Interruption
    d. Fabrication
11. Which of the following is not a classic data security requirement?
    a. Confidentiality
    b. Integrity
    c. Availability
    d. Authentication
12. _____ requirements ensure the privacy of data.
    a. Confidentiality
    b. Integrity
    c. Availability
    d. Authentication
13. _____ requirements ensure that data and programs are changed in an authorized manner.
    a. Confidentiality
    b. Integrity
    c. Availability
    d. Authentication
14. _____ requirements ensure the proper functioning of all systems such that there is no denial of service to authorized users.
    a. Integrity
    b. Availability
    c. Authentication
    d. Non-repudiation
15. _____ requirements ensure that the message is from the source it claims to be from.
    a. Integrity
    b. Availability
    c. Authentication
    d. Non-repudiation
16. _____ requirements prevent an individual or entity from denying having performed a particular action related to data.
    a. Integrity
    b. Availability
    c. Authentication
    d. Non-repudiation
17. In the area of information system security, integrity is related to _____ factor(s).
    a. intrinsic
    b. extrinsic
    c. both intrinsic and extrinsic
    d. none of the above
18. Mechanisms to ensure integrity fall into _____ broad classes.
    a. two
    b. three
    c. four
    d. five
19. _____ mechanisms seek to maintain integrity by blocking unauthorized attempts to change data.

Access Complete Test Bank for Information Security Text and Cases 2nd Dhillon

a. Prevention
b. Intrusion
c. Detection
d. Correction

20. _____ mechanisms simply report violations of integrity.
    a. Prevention
    b. Intrusion
    c. Detection
    d. Correction
21. _____ mechanisms analyze data to see if the required security constraints still hold.
    a. Prevention
    b. Intrusion
    c. Detection
    d. Correction
22. The concept of _____ has often been equated to disaster recovery and contingency planning.
    a. confidentiality
    b. integrity
    c. availability
    d. authentication
23. Escrow, redundancy, backup, and recovery plans are controls to ensure _____ requirements.
    a. confidentiality
    b. integrity
    c. availability
    d. authentication
24. Hash total, check bits, pedigree checks, and vendor assurance sequencing are controls to ensure _____ requirements.
    a. confidentiality
    b. integrity
    c. availability
    d. authentication
25. Encryption, copyright, and patents are controls to ensure _____ requirements.
    a. confidentiality
    b. integrity
    c. availability
    d. authentication
26. Timeliness is an important attribute of _____, since obsolete data are not necessarily true and correct.
    a. confidentiality
    b. integrity
    c. availability
    d. authenticity
27. Audit logs, verification validation, vendor assurances, and serial checks are controls to ensure _____ requirements.
    a. confidentiality
    b. integrity
    c. availability
    d. authentication
28. The importance of _____ as an information system security requirement came about because of increased reliance on electronic communications and maintaining the legality of certain types of electronic documents.

Access Complete Test Bank for Information Security Text and Cases 2nd Dhillon

a. integrity
b. availability
c. authentication
d. non-repudiation

29. Within the information system security domain, _____ has been defined as a property achieved through cryptographic methods.
    a. integrity
    b. availability
    c. authentication
    d. non-repudiation
30. Good testing, coding, and maintenance are the cornerstones of _____ controls.
    a. software development
    b. operating system
    c. program
    d. data

Answer Key

1. b	7. c	13. b	19. a	25. a
2. d	8. d	14. b	20. c	26. d
3. b	9. c	15. c	21. c	27. d
4. c	10.d	16. d	22. c	28. d
5. a	11. d	17. c	23. c	29. d
6. b	12. a	18. a	24. b	30. a

Access Complete Test Bank for Information Security Text and Cases 2nd Dhillon