**Security Fundamentals**

1Which of the following contains the primary goals and objectives of

security?

A. A network’s border perimeter

B. The CIA Triad

C. A stand-alone system

D. The Internet

2. Vulnerabilities and risks are evaluated based on their threats

against which of the following?

A. One or more of the CIA Triad principles

B. Data usefulness

C. Due care

D. Extent of liability

3. Which of the following is a principle of the CIA Triad that means

authorized subjects are granted timely and uninterrupted access to

objects?

A. Identification

B. Availability

C. Encryption

D. Layering

4. Which of the following is *not* considered a violation of

confidentiality?

A. Stealing passwords

B. Eavesdropping

C. Hardware destruction

D. Social engineering

5. Which of the following is not true?

A. Violations of confidentiality include human error.

B. Violations of confidentiality include management oversight.

C. Violations of confidentiality are limited to direct intentional

attacks.

D. Violations of confidentiality can occur when a transmission is

not properly encrypted.

6. STRIDE is often used in relation to assessing threats against

applications or operating systems. Which of the following is not an

element of STRIDE?

A. Spoofing

B. Elevation of privilege

C. Repudiation

D. Disclosure

7. If a security mechanism offers availability, then it offers a high

level of assurance that authorized subjects can

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ the data, objects, and

resources.

A. Control

B. Audit

C. Access

D. Repudiate

8. \_\_\_\_\_\_\_\_\_\_\_\_ refers to keeping information confidential that is

personally identifiable or which might cause harm,

embarrassment, or disgrace to someone if revealed.

A. Seclusion

B. Concealment

C. Privacy

D. Criticality

9. All but which of the following items requires awareness for all

individuals affected?

A. Restricting personal email

B. Recording phone conversations

C. Gathering information about surfing habits

D. The backup mechanism used to retain email messages

10. What element of data categorization management can override all

other forms of access control?

A. Classification

B. Physical access

C. Custodian responsibilities

D. Taking ownership

11. What ensures that the subject of an activity or event cannot deny

that the event occurred?

A. CIA Triad

B. Abstraction

C. Nonrepudiation

D. Hash totals

12. Which of the following is the most important and distinctive

concept in relation to layered security?

A. Multiple

B. Series

C. Parallel

D. Filter

13. Which of the following is *not* considered an example of data

hiding?

A. Preventing an authorized reader of an object from deleting that

object

B. Keeping a database from being accessed by unauthorized

visitors

C. Restricting a subject at a lower classification level from

accessing data at a higher classification level

D. Preventing an application from accessing hardware directly

14. What is the primary goal of change management?

A. Maintaining documentation

B. Keeping users informed of changes

C. Allowing rollback of failed changes

D. Preventing security compromises

15. What is the primary objective of data classification schemes?

A. To control access to objects for authorized subjects

B. To formalize and stratify the process of securing data based on

assigned labels of importance and sensitivity

C. To establish a transaction trail for auditing accountability

D. To manipulate access controls to provide for the most efficient

means to grant or restrict functionality

16. Which of the following is typically *not* a characteristic considered

when classifying data?

A. Value

B. Size of object

C. Useful lifetime

D. National security implications

17. What are the two common data classification schemes?

A. Military and private sector

B. Personal and government

C. Private sector and unrestricted sector

D. Classified and unclassified

18. Which of the following is the lowest military data classification for

classified data?

A. Sensitive

B. Secret

C. Proprietary

D. Private

19. Which commercial business/private sector data classification is

used to control information about individuals within an

organization?

A. Confidential

B. Private

C. Sensitive

D. Proprietary

20. Data classifications are used to focus security controls over all but

which of the following?

A. Storage

B. Processing

C. Layering

D. Transfer

\*\*\*\***ANSWERS**

1. B. The primary goals and objectives of security are confidentiality,

integrity, and availability, commonly referred to as the *CIA Triad*.

2. A. Vulnerabilities and risks are evaluated based on their threats

against one or more of the CIA Triad principles.

3. B. Availability means that authorized subjects are granted timely

and uninterrupted access to objects.

4. C. Hardware destruction is a violation of availability and possibly

integrity. Violations of confidentiality include capturing network

traffic, stealing password files, social engineering, port scanning,

shoulder surfing, eavesdropping, and sniffing.

5. C. Violations of confidentiality are not limited to direct intentional

attacks. Many instances of unauthorized disclosure of sensitive or

confidential information are due to human error, oversight, or

ineptitude.

6. D. Disclosure is not an element of STRIDE. The elements of

STRIDE are spoofing, tampering, repudiation, information

disclosure, denial of service, and elevation of privilege.

7. C. Accessibility of data, objects, and resources is the goal of

availability. If a security mechanism offers availability, then it is

highly likely that the data, objects, and resources are accessible to

authorized subjects.

8. C. Privacy refers to keeping information confidential that is

personally identifiable or which might cause harm,

embarrassment, or disgrace to someone if revealed. Seclusion is to

store something in an out of the way location. Concealment is the

act of hiding or preventing disclosure. The level to which

information is mission critical is its measure of criticality.

9. D. Users should be aware that email messages are retained, but the

backup mechanism used to perform this operation does not need

to be disclosed to them.

10. D. Ownership grants an entity full capabilities and privileges over

the object they own. The ability to take ownership is often granted

to the most powerful accounts in an operating system because it

can be used to overstep any access control limitations otherwise

implemented.

11. C. Nonrepudiation ensures that the subject of an activity or event

cannot deny that the event occurred.

12. B. Layering is the deployment of multiple security mechanisms in a

series. When security restrictions are performed in a series, they

are performed one after the other in a linear fashion. Therefore, a

single failure of a security control does not render the entire

solution ineffective.

13. A. Preventing an authorized reader of an object from deleting that

object is just an example of access control, not data hiding. If you

can read an object, it is not hidden from you.

14. D. The prevention of security compromises is the primary goal of

change management.

15. B. The primary objective of data classification schemes is to

formalize and stratify the process of securing data based on

assigned labels of importance and sensitivity.

16. B. Size is not a criterion for establishing data classification. When

classifying an object, you should take value, lifetime, and security

implications into consideration.

17. A. Military (or government) and private sector (or commercial

business) are the two common data classification schemes.

18. B. Of the options listed, secret is the lowest classified military data

classification. Keep in mind that items labeled as confidential,

secret, and top secret are collectively known as classified, and

confidential is below secret in the list.

19. B. The commercial business/private sector data classification of

private is used to protect information about individuals.

20. C. Layering is a core aspect of security mechanisms, but it is not a

focus of data classifications.

**Personnel Security and Risk Management**

Which of the following is the weakest element in any security

solution?

A. Software products

B. Internet connections

C. Security policies

D. Humans

2. When seeking to hire new employees, what is the first step?

A. Create a job description.

B. Set position classification.

C. Screen candidates.

D. Request resumes.

3. Which of the following is a primary purpose of an exit interview?

A. To return the exiting employee’s personal belongings

B. To review the nondisclosure agreement

C. To evaluate the exiting employee’s performance

D. To cancel the exiting employee’s network access accounts

4. When an employee is to be terminated, which of the following

should be done?

A. Inform the employee a few hours before they are officially

terminated.

B. Disable the employee’s network access just as they are informed

of the termination.

C. Send out a broadcast email informing everyone that a specific

employee is to be terminated.

D. Wait until you and the employee are the only people remaining

in the building before announcing the termination.

5. If an organization contracts with outside entities to provide key

business functions or services, such as account or technical

support, what is the process called that is used to ensure that these

entities support sufficient security?

A. Asset identification

B. Third-party governance

C. Exit interview

D. Qualitative analysis

6. A portion of the \_\_\_\_\_\_\_\_\_\_\_\_\_\_ is the logical and practical

investigation of business processes and organizational policies.

This process/policy review ensures that the stated and

implemented business tasks, systems, and methodologies are

practical, efficient, cost-effective, but most of all (at least in relation

to security governance) that they support security through the

reduction of vulnerabilities and the avoidance, reduction, or

mitigation of risk.

A. Hybrid assessment

B. Risk aversion process

C. Countermeasure selection

D. Documentation review

7. Which of the following statements is *not* true?

A. IT security can provide protection only against logical or

technical attacks.

B. The process by which the goals of risk management are

achieved is known as risk analysis.

C. Risks to an IT infrastructure are all computer based.

D. An asset is anything used in a business process or task.

8. Which of the following is *not* an element of the risk analysis

process?

A. Analyzing an environment for risks

B. Creating a cost/benefit report for safeguards to present to

upper management

C. Selecting appropriate safeguards and implementing them

D. Evaluating each threat event as to its likelihood of occurring

and cost of the resulting damage

9. Which of the following would generally *not* be considered an asset

in a risk analysis?

A. A development process

B. An IT infrastructure

C. A proprietary system resource

D. Users’ personal files

10. Which of the following represents accidental or intentional

exploitations of vulnerabilities?

A. Threat events

B. Risks

C. Threat agents

D. Breaches

11. When a safeguard or a countermeasure is not prese

nt or is not

sufficient, what remains?

A. Vulnerability

B. Exposure

C. Risk

D. Penetration

12. Which of the following is *not* a valid definition for risk?

A. An assessment of probability, possibility, or chance

B. Anything that removes a vulnerability or protects against one or

more specific threats

C. Risk = threat \* vulnerability

D. Every instance of exposure

13. When evaluating safeguards, what is the rule that should be

followed in most cases?

A. The expected annual cost of asset loss should not exceed the

annual costs of safeguards.

B. The annual costs of safeguards should equal the value of the

asset.

C. The annual costs of safeguards should not exceed the expected

annual cost of asset loss.

D. The annual costs of safeguards should not exceed 10 percent of

the security budget.

14. How is single loss expectancy (SLE) calculated?

A. Threat + vulnerability

B. Asset value ($) \* exposure factor

C. Annualized rate of occurrence \* vulnerability

D. Annualized rate of occurrence \* asset value \* exposure factor

15. How is the value of a safeguard to a company calculated?

A. ALE before safeguard - ALE after implementing the safeguard -

annual cost of safeguard

B. ALE before safeguard \* ARO of safeguard

C. ALE after implementing safeguard + annual cost of safeguard -

controls gap

D. Total risk - controls gap

16. What security control is directly focused on preventing collusion?

A. Principle of least privilege

B. Job descriptions

C. Separation of duties

D. Qualitative risk analysis

17. What process or event is typically hosted by an organization and is

targeted to groups of employees with similar job functions?

A. Education

B. Awareness

C. Training

D. Termination

18. Which of the following is *not* specifically or directly related to

managing the security function of an organization?

A. Worker job satisfaction

B. Metrics

C. Information security strategies

D. Budget

19. While performing a risk analysis, you identify a threat of fire and a

vulnerability because there are no fire extinguishers. Based on this

information, which of the following is a possible risk?

A. Virus infection

B. Damage to equipment

C. System malfunction

D. Unauthorized access to confidential information

20. You’ve performed a basic quantitative risk analysis on a specific

threat/vulnerability/risk relation. You select a possible

countermeasure. When performing the calculations again, which of

the following factors will change?

a. Exposure factor

b. Single loss expectancy

c. Asset value

d. Annualized rate of occurrence

**\*\*\*\*Answers**

1. D. Regardless of the specifics of a security solution, humans are the

weakest element.

2. A. The first step in hiring new employees is to create a job

description. Without a job description, there is no consensus on

what type of individual needs to be found and hired.

3. B. The primary purpose of an exit interview is to review the

nondisclosure agreement (NDA) and other liabilities and

restrictions placed on the former employee based on the

employment agreement and any other security-related

documentation.

4. B. You should remove or disable the employee’s network user

account immediately before or at the same time they are informed

of their termination.

5. B. Third-party governance is the application of security oversight

on third parties that your organization relies on.

6. D. A portion of the documentation review is the logical and

practical investigation of business processes and organizational

policies.

7. C. Risks to an IT infrastructure are not all computer based. In fact,

many risks come from noncomputer sources. It is important to

consider all possible risks when performing risk evaluation for an

organization. Failing to properly evaluate and respond to all forms

of risk, a company remains vulnerable.

8. C. Risk analysis includes analyzing an environment for risks,

evaluating each threat event as to its likelihood of occurring and

the cost of the damage it would cause, assessing the cost of various

countermeasures for each risk, and creating a cost/benefit report

for safeguards to present to upper management. Selecting

safeguards is a task of upper management based on the results of

risk analysis. It is a task that falls under risk management, but it is

not part of the risk analysis process.

9. D. The personal files of users are not usually considered assets of

the organization and thus are not considered in a risk analysis.

10. A. Threat events are accidental or intentional exploitations of

vulnerabilities.

11. A. A vulnerability is the absence or weakness of a safeguard or

countermeasure.

12. B. Anything that removes a vulnerability or protects against one or

more specific threats is considered a safeguard or a

countermeasure, not a risk.

13. C. The annual costs of safeguards should not exceed the expected

annual cost of asset loss.

14. B. SLE is calculated using the formula SLE = asset value ($) \*

exposure factor (SLE = AV \* EF).

15. A. The value of a safeguard to an organization is calculated by ALE

before safeguard – ALE after implementing the safeguard – annual

cost of safeguard [(ALE1 – ALE2) – ACS].

16. C. The likelihood that a co-worker will be willing to collaborate on

an illegal or abusive scheme is reduced because of the higher risk of

detection created by the combination of separation of duties,

restricted job responsibilities, and job rotation.

17. C. Training is teaching employees to perform their work tasks and

to comply with the security policy. Training is typically hosted by

an organization and is targeted to groups of employees with similar

job functions.

18. A. Managing the security function often includes assessment of

budget, metrics, resources, information security strategies, and

assessing the completeness and effectiveness of the security

program.

19. B. The threat of a fire and the vulnerability of a lack of fire

extinguishers lead to the risk of damage to equipment.

20. D. A countermeasure directly affects the annualized rate of

occurrence, primarily because the countermeasure is designed to

prevent the occurrence of the risk, thus reducing its frequency per

year.