Chapter 1: An Overview of Information Security and Risk Management

TRUE/FALSE

1. An asset can be logical, such as a Web site, information, or data; or an asset can be physical, such as a person, computer system, or other tangible object.

   ANS: T PTS: 1 REF: 4

2. Intellectual property (IP) includes trade secrets, copyrights, trademarks, and patents.

   ANS: T PTS: 1 REF: 8

3. A Disaster Recovery Plan (DR plan) deals with identifying, classifying, responding to, and recovering from an incident.

   ANS: F PTS: 1 REF: 24

4. The vision of an organization is a written statement of an organization's purpose.

   ANS: F PTS: 1 REF: 31

5. An enterprise information security policy (EISP) addresses specific areas of technology and contains a statement on the organization's position on each specific area.

   ANS: F PTS: 1 REF: 31

MULTIPLE CHOICE

1. The ____ illustrates the most critical characteristics of information and has been the industry standard for computer security since the development of the mainframe.
   a. disaster recovery plan
   b. C.I.A. triangle
   c. strategic plan
   d. asset classification

   ANS: B PTS: 1 REF: 4

2. ____ ensures that only those with the rights and privileges to access information are able to do so.
   a. Confidentiality
   b. Availability
   c. Integrity
   d. Risk assessment

   ANS: A PTS: 1 REF: 4

3. Information assets have ____ when they are not exposed (while being stored, processed, or transmitted) to corruption, damage, destruction, or other disruption of their authentic states.
   a. risk assessment
   b. availability
   c. integrity
   d. confidentiality

   ANS: C PTS: 1 REF: 4

4. Information assets have ____ when authorized users - persons or computer systems - are able to access them in the specified format without interference or obstruction.
   a. integrity
   b. availability
   c. confidentiality
   d. risk assessment

ANS: B PTS: 1 REF: 4

5. A(n) ____ is an object, person, or other entity that is a potential risk of loss to an asset.
   a. payload
   b. intellectual property
   c. Trojan horse
   d. threat

   ANS: D PTS: 1 REF: 4

6. The term ____ refers to a broad category of electronic and human activities in which an unauthorized individual gains access to the information an organization is trying to protect.
   a. theft
   b. trespass
   c. polymorphism
   d. denial-of-service

   ANS: B PTS: 1 REF: 5

7. A ____ attack seeks to deny legitimate users access to services by either tying up a server's available resources or causing it to shut down.
   a. Trojan horse
   b. DoS
   c. social engineering
   d. spyware

   ANS: B PTS: 1 REF: 6

8. ____ hack systems to conduct terrorist activities through network or Internet pathways.
   a. Cyberterrorists
   b. Script kiddies
   c. Programmers
   d. Social engineers

   ANS: A PTS: 1 REF: 9

9. ____ is the process of examining, documenting, and assessing the security posture of an organization's information technology and the risks it faces.
   a. Risk identification
   b. Data classification
   c. Security clearance
   d. DR

   ANS: A PTS: 1 REF: 12

10. ____ assigns a risk rating or score to each information asset. Although this number does not mean anything in absolute terms, it is useful in gauging the relative risk to each vulnerable information asset and facilitates the development of comparative ratings later in the risk control process.
    a. BC
    b. Risk assessment
    c. DR
    d. Avoidance

    ANS: B PTS: 1 REF: 18

11. ____ (sometimes referred to as avoidance) is the risk control strategy that attempts to prevent the exploitation of a vulnerability.
    a. Acceptance
    b. Transference
    c. Defense
    d. Mitigation

    ANS: C PTS: 1 REF: 21

12. ____ is a risk control approach that attempts to shift the risk to other assets, other processes, or other organizations.
    a. Transference
    b. Mitigation
    c. Acceptance
    d. Avoidance

    ANS: A PTS: 1 REF: 21

13. ____ is the risk control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.
    a. Avoidance
    b. Transference
    c. Acceptance
    d. Mitigation

    ANS: D PTS: 1 REF: 22

14. ____ of risk is the choice to do nothing to protect an information asset and to accept the outcome of its potential exploitation.
    a. Inheritance
    b. Acceptance
    c. Avoidance
    d. Mitigation

    ANS: B PTS: 1 REF: 22

15. A(n) ____ is used to anticipate, react to, and recover from events that threaten the security of information and information assets in an organization; it is also used to restore the organization to normal modes of business operations;
    a. threat plan
    b. social plan
    c. contingency plan
    d. security plan

    ANS: C PTS: 1 REF: 23

16. A(n) ____ is an investigation and assessment of the impact that various attacks can have on the organization.
    a. business impact analysis (BIA)
    b. incident response analysis (IRA)
    c. business continuity analysis (BCA)
    d. threat analysis

    ANS: A PTS: 1 REF: 23

17. A(n) ____ is any clearly identified attack on the organization's information assets that would threaten the assets' confidentiality, integrity, or availability.
    a. trespass
    b. Trojan horse
    c. risk
    d. incident

    ANS: D PTS: 1 REF: 23-24

18. A ____ deals with the preparation for and recovery from a disaster, whether natural or man-made.
    a. mitigation plan
    b. disaster recovery plan
    c. risk management
    d. risk assessment

    ANS: B PTS: 1 REF: 24

19. A ____ is a document that describes how, in the event of a disaster, critical business functions continue at an alternate location while the organization recovers its ability to function at the primary site.
    a. risk assessment plan
    b. business continuity plan
    c. incident response plan
    d. disaster recovery plan

    ANS: B PTS: 1 REF: 25

20. A(n) ____ is a plan or course of action used by an organization to convey instructions from its senior management to those who make decisions, take actions, and perform other duties on behalf of the organization.
    a. policy
    b. assessment
    c. business continuity plan
    d. residual risk

ANS: A PTS: 1 REF: 30

21. ____ is the process of moving an organization toward its vision.
    a. Security planning
    b. Contingency planning
    c. Strategic planning
    d. Enterprise information planning

    ANS: C PTS: 1 REF: 31

COMPLETION

1. _____ is defined by the Committee on National Security Systems (CNSS) as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

   ANS: Information security

   PTS: 1 REF: 3

2. A(n) _____ is defined as a "flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or violation of the system's security policy."

   ANS: vulnerability

   PTS: 1 REF: 4

3. _____ is the process of applying controls to reduce the risks to an organization's data and information systems.

   ANS: Risk control

   PTS: 1 REF: 12

4. _____ is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of all the components of the organization's information system.

   ANS: Risk management

   PTS: 1 REF: 13

5. For the purpose of making relative risk assessments, we can say that _____ equals the likelihood of a vulnerability occurring times the value (or impact) of that asset to the organization minus the percentage of risk that is already being controlled plus an element of uncertainty.

   ANS: risk

   PTS: 1 REF: 19

MATCHING

Match each item with a statement below.

a. Threat agent
f. Risk management

b. Exploit
c. Hacker
d. Virus
e. Trojan horse
g. Likelihood
h. Residual risk
i. Standard

1. A specific and identifiable instance of a general threat
2. A detailed statement of what must be done to comply with policy
3. A person who bypasses legitimate controls on an information system to gain access illegally
4. Something that looks like a desirable program or tool, but that is in fact a malicious entity
5. The probability that a specific vulnerability within an organization will be successfully attacked
6. The risk that remains to an information asset even after an existing control has been applied
7. A means to target a specific vulnerability
8. The process used to identify and then control risks to an organization's information assets
9. A segment of code that performs malicious actions

1. ANS: A PTS: 1 REF: 4
2. ANS: I PTS: 1 REF: 30
3. ANS: C PTS: 1 REF: 6
4. ANS: E PTS: 1 REF: 7
5. ANS: G PTS: 1 REF: 18
6. ANS: H PTS: 1 REF: 20
7. ANS: B PTS: 1 REF: 5
8. ANS: F PTS: 1 REF: 12
9. ANS: D PTS: 1 REF: 6

SHORT ANSWER

1. What is a polymorphic threat?

   ANS:
   A polymorphic threat is one that changes its apparent shape over time, making it undetectable by techniques that look for preconfigured signatures. These viruses and worms actually evolve, changing their size and appearance to elude detection by antivirus software programs. This means that an e-mail generated by the virus may not match previous examples, making detection more of a challenge.

   PTS: 1 REF: 7

2. During an information asset valuation, what questions should be asked as each asset is assigned to a category?

   ANS:
   As each asset is assigned to a category, the following questions should be asked:

   - Is this asset the most critical to the organization's success?
   - Does it generate the most revenue?
   - Does it generate the most profit?
   - Would it be the most expensive to replace?
   - Will it be the most expensive to protect?
   - If revealed, would it cause the most embarrassment or greatest damage? Does the law or other regulation require us to protect this asset?

PTS: 1 REF: 15

3. Once the project team for information security development has created a ranked vulnerability worksheet, it must choose one of five approaches for controlling the risks that result from the vulnerabilities. List the five approaches.

   ANS:
   The five approaches are:
   - Defense
   - Transferal
   - Mitigation
   - Acceptance
   - Termination

   PTS: 1 REF: 21

4. Of the five major risk control strategies discussed in this chapter, which is the preferred strategy when it can be applied? Give some examples of techniques used in this approach.

   ANS:
   The defense approach attempts to prevent the exploitation of a vulnerability. This is the preferred approach and is accomplished by means of countering threats, removing vulnerabilities in assets, limiting access to assets, and adding protective safeguards.

   PTS: 1 REF: 21

5. Describe the transference approach to risk control and give three specific examples of risk transfer.

   ANS:
   The risk transference approach attempts to shift the risk to other assets, other processes, or other organizations. This may be accomplished through rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or implementing service contracts with providers.

   PTS: 1 REF: 21

6. What are the typical subordinate functions of contingency planning?

   ANS:
   Contingency planning typically involves four subordinate functions:

   - Business impact analysis (BIA)
   - Incident response planning (IRP)
   - Disaster recovery planning (DRP)
   - Business continuity planning (BCP)

   PTS: 1 REF: 23

7. Provide a brief summary of the three main steps involved in contingency planning.

   ANS:

1. The IR plan focuses on immediate response, but if the event escalates or is disastrous (such as a fire, flood, earthquake, or total blackout), the process moves on to disaster recovery and business continuity.

2. The DR plan typically focuses on restoring systems at the original site after disasters occur and, as such, is closely associated with the BC plan.

3. The BC occurs concurrently with DR plan when the damage is major or long term, requiring more than simple restoration of information and information resources. The BCP establishes critical business functions at an alternate site.

PTS: 1 REF: 25

8. How is a business continuity (BC) plan different than a disaster recovery (DR) plan?

ANS:
A disaster recovery (DR) plan typically focuses on restoring systems at the original site after disasters occur and, as such, is closely associated with the business continuity (BC) plan. The BC plan occurs concurrently with the DR plan with the damage is major or long term, requiring more than simple restoration of information and information resources. The BC plan establishes critical business functions at an alternate site.

PTS: 1 REF: 25

9. Provide brief descriptions for access control lists (ACLs) and configuration rules.

ANS:
Access control lists (ACLs): Lists, matrices, and capability tables governing the rights and privileges of particular users to a particular systems.

Configuration rules: The specific configuration codes entered into security systems to guide the execution of the system when information is passing through it.

PTS: 1 REF: 33

10. What are five key elements that a security policy should have in order to remain viable over time?

ANS:
- An individual (such as a policy administrator) responsible for the creation, revision, distribution, and storage of the policy; this individual should solicit input from all communities of interest in policy development

- A schedule of reviews to ensure currency and accuracy, and to demonstrate due diligence

- A mechanism by which individuals can comfortably make recommendations for revisions, preferably anonymously

- A policy and revision date and possibly a “sunset” expiration date

- Optionally, policy management software to streamline the steps of writing the policy, tracking the workflow of policy approvals, publishing the policy once it is written and approved, and tracking when individuals have read the policy

PTS: 1 REF: 34