Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following items are defined by policies?

   A. Rules
   B. Expectations
   C. Patterns of behavior
   D. All of the above

2. Without policy, human beings would live in a state of _____.

   A. chaos
   B. bliss
   C. harmony
   D. laziness

3. A guiding principle is best described as which of the following?

   A. A financial target
   B. A fundamental philosophy or belief
   C. A regulatory requirement
   D. A person in charge

4. Which of the following best describes corporate culture?

   A. Shared attitudes, values, and goals
   B. Multiculturalism
   C. A requirement to all act the same
   D. A religion

5. The responsibilities associated with the policy life cycle process are distributed throughout an organization. During the "develop" phase of the cybersecurity policy life cycle, the board of directors and/or executive management are responsible for which of the following?

   A. Communicating guiding principles and authorizing the policy
   B. Separating religion from policy
   C. Monitoring and evaluating any policies
   D. Auditing the policy

6. Which of the following best describes the role of policy?

   A. To codify guiding principles
   B. To shape behavior
   C. To serve as a roadmap
   D. All of the above

7. A cybersecurity policy is a directive that defines which of the following?

   A. How employees should do their jobs
   B. How to pass an annual audit
   C. How an organization protects information assets and systems against cyber attacks and nonmalicious incidents
   D. How much security insurance a company should have

8. Which of the following is not an example of an information asset?

   A. Customer financial records
   B. Marketing plan
   C. Patient medical history
   D. Building graffiti

9. What are the seven characteristics of a successful policy?

   A. Endorsed, relevant, realistic, cost-effective, adaptable, enforceable, inclusive
   B. Endorsed, relevant, realistic, attainable, adaptable, enforceable, inclusive
   C. Endorsed, relevant, realistic, technical, adaptable, enforceable, inclusive
   D. Endorsed, relevant, realistic, legal, adaptable, enforceable, inclusive

10. A policy that has been endorsed has the support of which of the following?

    A. Customers
    B. Creditors
    C. The union
    D. Management

11. Who should always be exempt from policy requirements?

- **A.** Employees
- **B.** Executives
- **C.** No one
- **D.** Salespeople

12. "Attainable" means that the policy _____.

- **A.** can be successfully implemented
- **B.** is expensive
- **C.** only applies to suppliers
- **D.** must be modified annually

13. Which of the following statements is always true?

- **A.** Policies stifle innovation.
- **B.** Policies make innovation more expensive.
- **C.** Policies should be adaptable.
- **D.** Effective policies never change.

14. If a cybersecurity policy is violated and there is no consequence, the policy is considered to be which of the following?

- **A.** Meaningless
- **B.** Inclusive
- **C.** Legal
- **D.** Expired

15. Who must approve the retirement of a policy?

- **A.** A compliance officer
- **B.** An auditor
- **C.** Executive management or the board of directors
- **D.** Legal counsel

16. Which of the following sectors is not considered part of the "critical infrastructure"?

    A. Public health
    B. Commerce
    C. Banking
    D. Museums and arts

17. Which term best describes government intervention with the purpose of causing a specific set of actions?

    A. Deregulation
    B. Politics
    C. Regulation
    D. Amendments

18. The objectives of GLBA and HIPAA, respectively, are to protect _____.

    A. financial and medical records
    B. financial and credit card records
    C. medical and student records
    D. judicial and medical records

19. Which of the following states was the first to enact consumer breach notification?

    A. Kentucky
    B. Colorado
    C. Connecticut
    D. California

20. Which of the following terms best describes the process of developing, publishing, adopting, and reviewing a policy?

    A. Policy two-step
    B. Policy aging
    C. Policy retirement
    D. Policy life cycle

21. Who should be involved in the process of developing cybersecurity policies?

- **A.** Only upper-management-level executives
- **B.** Only part-time employees
- **C.** Personnel throughout the company
- **D.** Only outside, third-party consultants

22. Which of the following does *not* happen in the policy development phase?

- **A.** Planning
- **B.** Enforcement
- **C.** Authorization
- **D.** Approval

23. Which of the following occurs in the policy publication phase?

- **A.** Communication
- **B.** Policy dissemination
- **C.** Education
- **D.** All of the above

24. How often should policies be reviewed?

- **A.** Never
- **B.** Only when there is a significant change
- **C.** Annually
- **D.** At least annually, or sooner if there is a significant change

25. Normative integration is the goal of the adoption phase. This means _____.

- **A.** There are no exceptions to the policy
- **B.** The policy passes the stress test
- **C.** The policy becomes expected behavior, all others being deviant
- **D.** The policy costs little to implement

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. The policy hierarchy is the relationships between which of the following?

   A. Guiding principles, regulations, laws, and procedures
   B. Guiding principles, standards, guidelines, and procedures
   C. Guiding principles, instructions, guidelines, and programs
   D. None of the above

2. Which of the following statements best describes the purpose of a standard?

   A. To state the beliefs of an organization
   B. To reflect the guiding principles
   C. To dictate mandatory requirements
   D. To make suggestions

3. Which of the following statements best describes the purpose of a guideline?

   A. To state the beliefs of an organization
   B. To reflect the guiding principles
   C. To dictate mandatory requirements
   D. To help people conform to a standard

4. Which of the following statements best describes the purpose of a baseline?

   A. To measure compliance
   B. To ensure uniformity across a similar set of devices
   C. To ensure uniformity and consistency
   D. To make suggestions

5. Simple Step, Hierarchical, Graphic, and Flowchart are examples of which of the following formats?

   A. Policy
   B. Program
   C. Procedure
   D. Standard

6. Which of the following terms best describes instructions and guidance on how to execute an initiative or how to respond to a situation, within a certain time frame, usually with defined stages and with designated resources?
   - **A.** Plan
   - **B.** Policy
   - **C.** Procedure
   - **D.** Package

7. Which of the following statements best describes a disadvantage to using the singular policy format?
   - **A.** The policy can be short.
   - **B.** The policy can be targeted.
   - **C.** You may end up with too many policies to maintain.
   - **D.** The policy can easily be updated.

8. Which of the following statements best describes a disadvantage to using the consolidated policy format?
   - **A.** Consistent language is used throughout the document.
   - **B.** Only one policy document must be maintained.
   - **C.** The format must include a composite management statement.
   - **D.** The potential size of the document.

9. Policies, standards, guidelines, and procedures should all be in the same document.
   - **A.** True
   - **B.** False
   - **C.** Only if the company is multinational
   - **D.** Only if the documents have the same author

10. Version control is the management of changes to a document and should include which of the following elements?
    - **A.** Version or revision number
    - **B.** Date of authorization or date that the policy took effect
    - **C.** Change description
    - **D.** All of the above

11. What is an exploit?
    - **A.** A phishing campaign
    - **B.** A malicious program or code designed to "exploit" or take advantage of a single vulnerability or set of vulnerabilities

C. A network or system weakness
D. A protocol weakness

12. The name of the policy, policy number, and overview belong in which of the following sections?

A. Introduction
B. Policy Heading
C. Policy Goals and Objectives
D. Policy Statement

13. The aim or intent of a policy is stated in the _____.

A. introduction
B. policy heading
C. policy goals and objectives
D. policy statement

14. Which of the following statements is true?

A. A security policy should include only one objective.
B. A security policy should not include any exceptions.
C. A security policy should not include a glossary.
D. A security policy should not list all step-by-step measures that need to be taken.

15. The _____ contains the rules that must be followed.

A. policy heading
B. policy statement
C. policy enforcement clause
D. policy goals and objectives

16. A policy should be considered _____.

A. mandatory
B. discretionary
C. situational
D. optional

17. Which of the following best describes policy definitions?

A. A glossary of terms, abbreviations, and acronyms used in the document that the reader may be unfamiliar with
B. A detailed list of the possible penalties associated with breaking rules set forth in the policy

C. A list of all the members of the security policy creation team

D. None of the above

18. The _____ contains the penalties that would apply if a portion of the security policy were to be ignored by an employee.

A. policy heading

B. policy statement

C. policy enforcement clause

D. policy statement of authority

19. What component of a security policy does the following phrase belong to? "Wireless networks are allowed only if they are separate and distinct from the corporate network."

A. Introduction

B. Administrative notation

C. The policy heading

D. The policy statement

20. There may be situations where it is not possible to comply with a policy directive. Where should the exemption or waiver process be explained?

A. Introduction

B. The policy statement

C. The policy enforcement clause

D. The policy exceptions

21. The name of the person/group (for example, executive committee) that authorized the policy should be included in _____.

A. the version control table or the policy statement

B. the heading or the policy statement

C. the policy statement or the policy exceptions

D. the version control table or the policy heading

22. When you're drafting a list of exceptions for a security policy, the language should _____.

A. be as specific as possible

B. be as vague as possible

C. reference another, dedicated document

D. None of the above

23. If supporting documentation would be of use to the reader, it should be _____.

    A. included in full in the policy document
    B. ignored because supporting documentation does not belong in a policy document
    C. listed in either the Policy Heading or Administrative Notation section
    D. included in a policy appendix

24. When writing a policy, standard, guideline, or procedure, you should use language that is _____.

    A. technical
    B. clear and concise
    C. legalese
    D. complex

25. Readers prefer "plain language" because it _____.

    A. helps them locate pertinent information
    B. helps them understand the information
    C. saves time
    D. All of the above

26. Which of the following is not a characteristic of plain language?

    A. Short sentences
    B. Using active voice
    C. Technical jargon
    D. Seven or fewer lines per paragraph

27. Which of the following terms is best to use when indicating a mandatory requirement?

    A. must
    B. shall
    C. should not
    D. may not

28. A company that uses the term "employees" to refer to workers who are on the company payroll should refer to them throughout their policies as _____.

    A. workforce members
    B. employees
    C. hired hands
    D. workers

29. Which of the following statements is true regarding policy definitions?
    A. They should be defined and maintained in a separate document.
    B. The general rule is to include definitions for any topics except technical, legal, or regulatory language.
    C. The general rule of policy definitions is to include definitions for any instance of industry-specific, technical, legal, or regulatory language.
    D. They should be created before any policy or standards.

30. Even the best-written policy will fail if which of the following is true?
    A. The policy is too long.
    B. The policy is mandated by the government.
    C. The policy doesn't have the support of management.
    D. All of the above.

EXERCISES

EXERCISE 2.1: Creating Standards, Guidelines, and Procedures

The University System has a policy that states, "All students must comply with their campus attendance standard."

1. You are tasked with developing a standard that documents the mandatory requirements (for example, how many classes can be missed without penalty). Include at least four requirements.
2. Create a guideline to help students adhere to the standard you created.
3. Create a procedure for requesting exemptions to the policy.

EXERCISE 2.2: Writing Policy Statements

1. Who would be the target audience for a policy related to campus elections?
2. Keeping in mind the target audience, compose a policy statement related to campus elections.
3. Compose an enforcement clause.

EXERCISE 2.3: Writing a Policy Introduction

1. Write an introduction to the policy you created in Exercise 2.2.
2. Generally an introduction is signed by an authority. Who would be the appropriate party to sign the introduction?
3. Write an exception clause.

Summary

Ensuring confidentiality, integrity, and availability is the unifying principle of every information security program. Collectively referred to as the ***CIA triad*** or ***CIA security model***, each attribute represents a fundamental objective and corresponding action related to the protection of information, processes, or systems. ***Confidentiality*** is protection from unauthorized access or disclosure. ***Integrity*** is protection from manipulation. ***Availability*** is protection from denial of service (DoS). In support of the CIA triad are the security principles known as the ***Five A's***: accountability, assurance, authentication, accounting, and authorization.

An ***information owner*** is one who has been assigned the authority and responsibility for ensuring that information and related systems are protected from creation through destruction. This includes making decisions on information classification, safeguards, and controls. ***Information custodians*** are those responsible for implementing, maintaining, and monitoring the safeguards based on decisions made by information owners. Cohesive decision making requires a framework.

A ***security framework*** is a collective term given to guidance on topics related to information systems security, predominantly regarding the planning, implementing, managing, and auditing of overall information security practices. In this chapter you learned highlights of ***NIST's Cybersecurity Framework***. Chapter 16 covers the NIST Cybersecurity Framework in detail. The ***International Organization for Standardization*** (ISO) has published a technology-neutral Code of Standards for Information Security known as the ISO/IEC 27002:2013. This standard has been internationally adopted by both private and public organizations of all sizes. ISO 27002:2013 is divided into 14 domains. Each of these categories has a control objective, compliance requirements, and recommended policy components. NIST has a number of Special Publications that complement the ISO Code of Practice. The publications provide in-depth research, recommendations, and guidance that can be applied to security domains and specific technologies. The ISO standards and the NIST Cybersecurity Framework could also be used by regulatory organizations to provide assurance that a cyber policy is robust and complete. In this book, we use both to build our information security policy and program.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following are the three principles in the CIA triad?

   A. Confidence, integration, availability
   B. Consistency, integrity, authentication
   C. Confidentiality, integrity, availability
   D. Confidentiality, integrity, awareness

2. Which of the following is an example of acting upon the goal of integrity?

   A. Ensuring that only authorized users can access data
   B. Ensuring that systems have 99.9% uptime
   C. Ensuring that all modifications go through a change-control process
   D. Ensuring that changes can be traced back to the editor

3. Which of the following is a control that relates to availability?

   A. Disaster recovery site
   B. Data loss prevention (DLP) system
   C. Training
   D. Encryption

4. Which of the following is an objective of confidentiality?

   A. Protection from unauthorized access
   B. Protection from manipulation
   C. Protection from denial of service
   D. Protection from authorized access

5. Which of the following is a good definition for confidentiality?

   A. The property that information is not made available or disclosed to unauthorized individuals, entities, or processes
   B. The processes, policies, and controls used to develop confidence that security measures are working as intended
   C. The positive identification of the person or system seeking access to secured information or systems
   D. The logging of access and usage of information resources

6. An important element of confidentiality is that all sensitive data needs to be controlled, audited, and monitored at all times. Which of the following provides an example about how data can be protected?

   A. Ensuring availability
   B. Encrypting data in transit and at rest
   C. Deploying faster servers
   D. Taking advantage of network programmability

7. Which of the following statements identify threats to availability? (Select all that apply.)

   A. Loss of processing capabilities due to natural disaster or human error
   B. Loss of confidentiality due to unauthorized access

C. Loss of personnel due to accident
D. Loss of reputation from unauthorized event

8. Which of the following terms best describes the logging of access and usage of information resources?

A. Accountability
B. Acceptance
C. Accounting
D. Actuality

9. Which of the following combinations of terms best describes the Five A's of information security?

A. Awareness, acceptance, availability, accountability, authentication
B. Awareness, acceptance, authority, authentication, availability
C. Accountability, assurance, authorization, authentication, accounting
D. Acceptance, authentication, availability, assurance, accounting

10. An information owner is responsible for _____.

A. maintaining the systems that store, process, and transmit information
B. protecting the business reputation and results derived from use of that information
C. protecting the people and processes used to access digital information
D. ensuring that information is protected, from creation through destruction

11. Which of the following terms best describes ISO?

A. Internal Standards Organization
B. International Organization for Standardization
C. International Standards Organization
D. Internal Organization of Systemization

12. Which of the following statements best describes opportunistic crime?

A. Crime that is well planned
B. Crime that is targeted
C. Crime that takes advantage of identified weaknesses or poorly protected information
D. Crime that is quick and easy

13. Which of the following terms best describes the motivation for hacktivism?

A. Financial
B. Political

C. Personal

E. Fun

14. The longer it takes a criminal to obtain unauthorized access, the _____

A. more time it takes

B. more profitable the crime is

C. better chance of success

D. better chance of getting caught

15. Which of the following terms best describes an attack whose purpose is to make a machine or network resource unavailable for its intended use?

A. Man-in-the-middle

B. Data breach

C. Denial of service

D. SQL injection

16. Information custodians are responsible for _____

A. writing policy

B. classifying data

C. approving budgets

D. implementing, maintaining, and monitoring safeguards

17. The National Institute of Standards and Technology (NIST) is a(n) _____

A. international organization

B. privately funded organization

C. U.S. government institution, part of the U.S. Department of Commerce

D. European Union agency

18. The International Organization for Standardization (ISO) is _____

A. a nongovernmental organization

B. an international organization

C. headquartered in Geneva

D. all of the above

19. The current ISO family of standards that relates to information security is _____.

A. BS 7799:1995

B. ISO 17799:2006

C. ISO/IEC 27000

D. None of the above

20. Which of the following terms best describes the security domain that relates to managing authorized access and preventing unauthorized access to information systems?

A. Security policy

B. Access control

C. Compliance

D. Risk assessment

21. Which of the following terms best describes the security domain that relates to how data is classified and valued?

A. Security policy

B. Asset management

C. Compliance

D. Access control

22. Which of the following terms best describes the security domain that includes HVAC, fire suppression, and secure offices?

A. Operations

B. Communications

C. Risk assessment

D. Physical and environmental controls

23. Which of the following terms best describes the security domain that aligns most closely with the objective of confidentiality?

A. Access control

B. Compliance

C. Incident management

D. Business continuity

24. The primary objective of the _____ domain is to ensure conformance with GLBA, HIPAA, PCI/DSS, and FERPA.

A. Security Policy

B. Compliance

C. Access Control

D. Contract and Regulatory

25. Processes that include responding to a malware infection, conducting forensics investigations, and reporting breaches are included in the _____ domain.

    A. Security Policy
    B. Operations and Communications
    C. Incident Management
    D. Business Continuity Management

26. Which of the following terms best describes a synonym for business continuity?

    A. Authorization
    B. Authentication
    C. Availability
    D. Accountability

27. Which domain focuses on service delivery, third-party security requirements, contractual obligations, and oversight?

    A. Incident Handling and Forensics
    B. Security Policy
    C. Supplier Relationships
    D. Information Security Incident Management

28. Which domain focuses on proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information?

    A. Cryptography
    B. Cryptanalysis
    C. Encryption and VPN Governance
    D. Legal and Compliance

29. Which domain focuses on integrating security into the employee life cycle, agreements, and training?

    A. Operations and Communications
    B. Human Resources Security Management
    C. Governance
    D. Legal and Compliance

30. Which of the following security objectives is most important to an organization?

    A. Confidentiality
    B. Integrity

C. Availability

D. The answer may vary from organization to organization

31. Which of the following are some of the components of NIST's Cybersecurity Framework core functions? (Choose all that apply.)

A. Identify

B. Integrity

C. Detect

D. Protect

E. All of the above

EXERCISES

EXERCISE 3.1: Understanding CIA

1. Define the security term "confidentiality." Provide an example of a business situation where confidentiality is required.
2. Define the security term "integrity." Provide an example of a business situation in which the loss of integrity could result in significant harm.
3. Define the security term "availability." Provide an example of a business situation in which availability is more important than confidentiality.

EXERCISE 3.2: Understanding Opportunistic Cybercrime

1. Define what is meant by an "opportunistic" crime.
2. Provide an example.
3. Locate (online) a copy of the most recent Verizon Data Breach Incident Report. What percentage of cybercrimes are considered "opportunistic"?

EXERCISE 3.3: Understanding Hacktivism or DDoS

1. Find a recent news article relating to either hacktivism or a distributed denial of service (DDoS) attack.
2. Summarize the attack.
3. Explain why the attacker was successful (or not).

mitigated. A *risk assessment* is used to calculate the level of risk. A number of publicly available risk assessment methodologies are available for organizations to use and customize. Risk acceptance indicates that the organization is willing to accept the level of risk associated with a given activity or process. Risk mitigation implies that one of four actions (or a combination of actions) will be undertaken: risk reduction, risk sharing, risk transference, or risk avoidance.

Risk management, governance, and information policy are the basis of an information program. Policies related to these domains include the following policies: Cybersecurity Policy, Cybersecurity Policy Authorization and Oversight, CISO, Cybersecurity Steering Committee, Cybersecurity Risk Management Oversight, Cybersecurity Risk Assessment, and Cybersecurity Risk Management.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. What does it indicate when a cybersecurity program is said to be "strategically aligned"?

   A. It supports business objectives.
   B. It adds value.
   C. It maintains compliance with regulatory requirements.
   D. All of the above.

2. How often should cybersecurity policies be reviewed?

   A. Once a year
   B. Only when a change needs to be made
   C. At a minimum, once a year and whenever there is a change trigger
   D. Only as required by law

3. Cybersecurity policies should be authorized by _____.

   A. the Board of Directors (or equivalent)
   B. business unit managers
   C. legal counsel
   D. stockholders

4. Which of the following statements best describes policies?

   A. Policies are the implementation of specifications.
   B. Policies are suggested actions or recommendations.
   C. Policies are instructions.
   D. Policies are the directives that codify organizational requirements.

5. Which of the following statements best represents the most compelling reason to have an employee version of the comprehensive cybersecurity policy?
   - **A.** Sections of the comprehensive policy may not be applicable to all employees.
   - **B.** The comprehensive policy may include unknown acronyms.
   - **C.** The comprehensive document may contain confidential information.
   - **D.** The more understandable and relevant a policy is, the more likely users will positively respond to it.

6. Which of the following is a common element of all federal cybersecurity regulations?
   - **A.** Covered entities must have a written cybersecurity policy.
   - **B.** Covered entities must use federally mandated technology.
   - **C.** Covered entities must self-report compliance.
   - **D.** Covered entities must notify law enforcement if there is a policy violation.

7. Organizations that choose to adopt the ISO 27002:2103 framework must _____.
   - **A.** use every policy, standard, and guideline recommended
   - **B.** create policies for every security domain
   - **C.** evaluate the applicability and customize as appropriate
   - **D.** register with the ISO

8. Evidence-based techniques used by cybersecurity auditors include which of the following elements?
   - **A.** Structured interviews, observation, financial analysis, and documentation sampling
   - **B.** Structured interviews, observation, review of practices, and documentation sampling
   - **C.** Structured interviews, customer service surveys, review of practices, and documentation sampling
   - **D.** Casual conversations, observation, review of practices, and documentation sampling

9. Which of the following statements best describes independence in the context of auditing?
   - **A.** The auditor is not an employee of the company.
   - **B.** The auditor is certified to conduct audits.
   - **C.** The auditor is not responsible for, has not benefited from, and is not in any way influenced by the audit target.
   - **D.** Each auditor presents his or her own opinion.

10. Which of the following states is *not* included in a CMM?
    - **A.** Average
    - **B.** Optimized

C. Ad hoc

D. Managed

11. Which of the following activities is not considered a governance activity?

A. Managing

B. Influencing

C. Evaluating

D. Purchasing

12. To avoid conflict of interest, the CISO could report to which of the following individuals?

A. The Chief Information Officer (CIO)

B. The Chief Technology Officer (CTO)

C. The Chief Financial Officer (CFO)

D. The Chief Compliance Officer (CCO)

13. Which of the following statements best describes the role of the Cybersecurity Steering Committee?

A. The committee authorizes policy.

B. The committee helps communicate, discuss, and debate on security requirements and business integration.

C. The committee approves the InfoSec budget.

D. None of the above.

14. Defining protection requirements is the responsibility of _____.

A. the ISO

B. the data custodian

C. data owners

D. the Compliance Officer

15. Designating an individual or team to coordinate or manage cybersecurity is required by _____.

A. GLBA

B. 23 NYCRR 500

C. PCI DSS

D. All of the above

16. Which of the following terms best describes the potential of an undesirable or unfavorable outcome resulting from a given action, activity, and/or inaction?

    A. Threat
    B. Risk
    C. Vulnerability
    D. Impact

17. Inherent risk is the state before _____.

    A. an assessment has been conducted
    B. security measures have been implemented
    C. the risk has been accepted
    D. None of the above

18. Which of the following terms best describes the natural, environmental, technical, or human event or situation that has the potential for causing undesirable consequences or impact?

    A. Risk
    B. Threat source
    C. Threat
    D. Vulnerability

19. Which of the following terms best describes a disgruntled employee with intent to do harm?

    A. Risk
    B. Threat source
    C. Threat
    D. Vulnerability

20. Which of the following activities is *not* considered an element of risk management?

    A. The process of determining an acceptable level of risk
    B. Assessing the current level of risk for a given situation
    C. Accepting the risk
    D. Installing risk-mitigation technologies and cybersecurity products

21. How much of the undesirable outcome the risk taker is willing to accept in exchange for the potential benefit is known as _____.

    A. risk acceptance
    B. risk tolerance
    C. risk mitigation
    D. risk avoidance

22. Which of the following statements best describes a vulnerability?

    A. A vulnerability is a weakness that could be exploited by a threat source.
    B. A vulnerability is a weakness that can never be fixed.
    C. A vulnerability is a weakness that can only be identified by testing.
    D. A vulnerability is a weakness that must be addressed regardless of the cost.

23. Which of the following are benefits of security controls?

    A. Detect threats
    B. Deter threats
    C. Prevent cyber-attacks and breaches
    D. All of the above

24. Which of the following is not a risk-mitigation action?

    A. Risk acceptance
    B. Risk sharing or transference
    C. Risk reduction
    D. Risk avoidance

25. Which of the following risks is best described as the expression of (the likelihood of occurrence after controls are applied) × (expected loss)?

    A. Inherent risk
    B. Expected risk
    C. Residual risk
    D. Accepted risk

26. Which of the following risk types best describes an example of insurance?

    A. Risk avoidance
    B. Risk transfer
    C. Risk acknowledgement
    D. Risk acceptance

27 Which of the following risk types relates to negative public opinion?

    A. Operational risk
    B. Financial risk
    C. Reputation risk
    D. Strategic risk

28. Which of the following is not true about compliance risk as it relates to federal and state regulations?

    A. Compliance risk cannot be avoided
    B. Compliance risk cannot be transferred
    C. Compliance risk cannot be accepted
    D. None of these answers are correct

29. Which of the following statements best describes organizations that are required to comply with multiple federal and state regulations?

    A. They must have different policies for each regulation.
    B. They must have multiple ISOs.
    C. They must ensure that their cybersecurity program includes all applicable requirements.
    D. They must choose the one regulation that takes precedence.

30. Which of the following are subcategories of the NIST Cybersecurity Framework that are related to cybersecurity governance?

    A. ID.GV-1: Organizational information security policy is established.
    B. ID.GV-2: Information security roles and responsibilities are coordinated and aligned with internal roles and external partners.
    C. ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
    D. ID.GV-4: Governance and risk management processes address cybersecurity risks.
    E. All of these answers are correct.

EXERCISES

EXERCISE 4-1: Understanding ISO 27002:2005

The introduction to ISO 27002:2005 includes this statement: "This International Standard may be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required."

1. Explain how this statement relates to the concept of strategic alignment.
2. The risk assessment domain was included in the ISO 27002:2005 edition and then removed in ISO 27002:2013. Why do you think they made this change?
3. What are the major topics of ISO 27005?

In this chapter, you learned that DLP is the technology and capability to detect any sensitive emails, documents, or information leaving your organization. This is often referred to as *data exfiltration* or *data extrusion*. Data exfiltration is the unauthorized transfer of data from a system or network manually (carried out by someone with physical access to such system), or it may be automated and carried out through malware or system compromise over a network.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following terms best describes a definable piece of information, stored in any manner, that is recognized as having value to the organization?

   A. NPPI
   B. Information asset
   C. Information system
   D. Classified data

2. Information systems _____, _____, and _____ information.

   A. create, modify, and delete
   B. classify, reclassify, and declassify
   C. store, process, and transmit
   D. use, label, and handle

3. Information owners are responsible for which of the following tasks?

   A. Classifying information
   B. Maintaining information
   C. Using information
   D. Registering information

4. Which of the following roles is responsible for implementing and maintaining security controls and reporting suspected incidents?

   A. Information owner
   B. Information vendor
   C. Information user
   D. Information custodian

5. FIPS-199 requires that federal government information and information systems be classified as _____.

   A. low, moderate, high security
   B. moderate, critical, low security
   C. high, critical, top-secret security
   D. none of the above

6. Information classification systems are used in which of the following organizations?

   A. Government
   B. Military
   C. Financial institutions
   D. All of the above

7. FIPS requires that information be evaluated for _____requirements with respect to the impact of unauthorized disclosure as well as the use of the information.

   A. integrity
   B. availability
   C. confidentiality
   D. secrecy

8. Which of the following National Security classifications requires the most protection?

   A. Secret
   B. Top Secret
   C. Confidential
   D. Unclassified

9. Which of the following National Security classifications requires the least protection?

   A. Secret
   B. Unclassified
   C. Confidential
   D. Sensitive But Unclassified (SBU)

10. The Freedom of Information Act (FOIA) allows anyone access to which of the following?

    A. Access to all government information just by asking
    B. Access to all classified documents

C. Access to classified documents on a "need to know" basis

D. Access to any records from federal agencies unless the documents can be officially declared exempt

11. Which of the following terms best describes the CIA attribute associated with the modification of information?

A. Classified

B. Integrity

C. Availability

D. Intelligence

12. Is it mandatory for all private businesses to classify information?

A. Yes.

B. Yes, but only if they want to pay less tax.

C. Yes, but only if they do business with the government.

D. No.

13. Which of the following is not a criterion for classifying information?

A. The information is not intended for the public domain.

B. The information has no value to the organization.

C. The information needs to be protected from those outside of the organization.

D. The information is subject to government regulations.

14. Data that is considered to be personal in nature and, if disclosed, is an invasion of privacy and a compromise of security is known as which of the following?

A. Nonpersonal public information

B. Nonprivate personal information

C. Nonpublic personal information

D. None of the above

15. Most organizations restrict access to protected, confidential, and internal-use data to which of the following roles within the organization?

A. Executives

B. Information owners

C. Users who have a "need to know"

D. Vendors

16. Labeling is the vehicle for communicating classification levels to which of the following roles within the organization?

    A. Employees
    B. Information custodians
    C. Contractors
    D. All of the above

17. Which of the following terms best describes rules for how to store, retain, and destroy data based on classification?

    A. Handling standards
    B. Classification procedures
    C. Use policies
    D. Material guidelines

18. Which of the following terms best describes the process of removing restricted classification levels?

    A. Declassification
    B. Classification
    C. Reclassification
    D. Negative classification

19. Which of the following terms best describes the process of upgrading or changing classification levels?

    A. Declassification
    B. Classification
    C. Reclassification
    D. Negative classification

20. The impact of destruction and/or permanent loss of information is used to determine which of the following safeguards?

    A. Authorization
    B. Availability
    C. Authentication
    D. Accounting

21. Which of the following terms best describes an example of a hardware asset?

    A. Server
    B. Database
    C. Operating system
    D. Radio waves

22. Which of the following statements best describes a MAC address?

    A. A MAC address is a dynamic network address.
    B. A MAC address is a unique host name.
    C. A MAC address is a unique hardware identifier.
    D. A MAC address is a unique alias.

23. 10.1.45.245 is an example of which of the following?

    A. A MAC address
    B. A host name
    C. An IP address
    D. An IP domain name

24. Source code and design documents are examples of which of the following?

    A. Software assets
    B. Proprietary information
    C. Internal-use classification
    D. Intellectual property (IP)

25. Which of the following terms best describes the act of classifying information based on an original classification decision already made by an authorized original classification authority?

    A. Reclassification
    B. Derivative classification
    C. Declassification
    D. Original classification

26. Which of the following types of information would not be considered NPPI?

    A. Social security number
    B. Date of birth
    C. Debit card PIN
    D. Car manufacturer's name

27. In keeping with best practices and regulatory expectations, legally protected data that is stored on mobile devices should be _____.

    A. masked
    B. encrypted
    C. labeled
    D. segregated

28. Which of the following statements best describes how written documents that contain NPPI should be handled?

    A. Written documents that contain NPPI should be stored in locked areas or in a locked cabinet.
    B. Written documents that contain NPPI should be destroyed by cross-cut shredding.
    C. Written documents that contain NPPI should be subject to company retention policies.
    D. All of the above.

29. Which of the following address types represents a device location on a network?

    A. A physical address
    B. A MAC address
    C. A logical address
    D. A static address

30. What is DLP?

    A. An email inspection technology used to prevent phishing attacks
    B. A software or solution for making sure that corporate users do not send sensitive or critical information outside the corporate network
    C. A web inspection technology used to prevent phishing attacks
    D. A cloud solution used to provide dynamic layer protection

EXERCISES

EXERCISE 5.1: Assigning Ownership

Owners are responsible for the protection of assets. For each of the following assets, assign an owner and list the owner's responsibilities in regard to protecting the asset:

1. The house you live in.
2. The car you drive.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following statements best describes the employee life cycle?

   A. The employee life cycle spans recruitment to career development.
   B. The employee life cycle spans onboarding to orientation.
   C. The employee life cycle spans user provision to termination.
   D. The employee life cycle spans recruitment to termination.

2. At which of the following phases of the hiring process should personnel security practices begin?

   A. Interview
   B. Offer
   C. Recruitment
   D. Orientation

3. A published job description for a web designer should not include which of the following?

   A. Job title
   B. Salary range
   C. Specifics about the web development tool the company is using
   D. Company location

4. Data submitted by potential candidates must be _____.

   A. protected as required by applicable law and organizational policy
   B. not protected unless the candidate is hired
   C. stored only in paper form
   D. publicly accessible

5. During the course of an interview, a job candidate should be given a tour of which of the following locations?

   A. The entire facility
   B. Public areas only (unless otherwise authorized)
   C. The server room
   D. The wiring closet

6. Which of the following facts is an interviewer permitted to reveal to a job candidate?
   - **A.** A detailed client list
   - **B.** The home phone numbers of senior management
   - **C.** The organization's security weaknesses
   - **D.** The duties and responsibilities of the position

7. Which of the following statements best describes the reason for conducting background checks?
   - **A.** To verify the truthfulness, reliability, and trustworthiness of the applicant
   - **B.** To find out if the applicant ever got in trouble in high school
   - **C.** To find out if the applicant has a significant other
   - **D.** To verify the applicant's hobbies, number of children, and type of house

8. Which of the following is not a background check type?
   - **A.** Credit history
   - **B.** Criminal history
   - **C.** Education
   - **D.** Religious or Political

9. Social media profiles often include gender, race, and religious affiliation. Which of the following statements best describes how this information should be used in the hiring process?
   - **A.** Gender, race, and religious affiliation can legally be used in making hiring decisions.
   - **B.** Gender, race, and religious affiliation cannot legally be used in making hiring decisions.
   - **C.** Gender, race, and religious affiliation are useful in making hiring decisions.
   - **D.** Gender, race, and religious affiliation listed in social media profiles should not be relied upon because they may be false.

10. Under the Fair Credit Reporting Act (FCRA), which of the following statements is true?
    - **A.** Employers cannot request a copy of an employee's credit report under any circumstances.
    - **B.** Employers must get the candidate's consent to request a credit report.
    - **C.** Employers cannot use credit information to deny a job.
    - **D.** Employers are required to conduct credit checks on all applicants.

11. Candidate and employee NPPI must be protected. NPPI does not include which of the following?
    - **A.** Social security number
    - **B.** Credit card number

C. Published telephone number

D. Driver's license number

12. Which of the following statements best describes the purpose of completing Department of Homeland Security/U.S. Citizenship and Immigration Services Form I-9 and providing supporting documentation?

A. The purpose is to establish identity and employment authorization.

B. The purpose is to determine tax identification and withholding.

C. The purpose is to document educational achievements.

D. The purpose is to verify criminal records.

13. The permissions and access rights a user is granted should match the user's role and responsibilities. Who is responsible for defining to whom access should be granted?

A. The data user

B. The data owner

C. The data custodian

D. The data author

14. Network administrators and help desk personnel often have elevated privileges. They are examples of which of the following roles?

A. The data owners

B. The data custodians

C. The data authors

D. The data sellers

15. Which of the following statements is *not* true of confidentiality agreements?

A. Confidentiality/nondisclosure agreements are legal protection against unauthorized use of information.

B. Confidentiality/nondisclosure agreements are generally considered a condition of work.

C. Confidentiality/nondisclosure agreements are legally binding contracts.

D. Confidentiality agreements should be required only of top-level executives.

16. Which of the following elements would you expect to find in an acceptable use agreement?

A. Handling standards

B. A lunch and break schedule

C. A job description

D. An evacuation plan

17. Which of the following statements best describes when acceptable use agreements should be reviewed, updated, and distributed?

    A. Acceptable use agreements should be reviewed, updated, and distributed only when there are organizational changes.
    B. Acceptable use agreements should be reviewed, updated, and distributed annually.
    C. Acceptable use agreements should be reviewed, updated, and distributed only during the merger and acquisition due diligence phase.
    D. Acceptable use agreements should be reviewed, updated, and distributed at the discretion of senior management.

18. Which of the following is true about the NICE Cybersecurity Workforce Framework (NICE Framework)?

    A. NICE is designed to provide guidance on how to implement the NIST Cybersecurity Framework.
    B. NICE is designed to provide guidance on how to identify, recruit, develop, and retain cybersecurity talent.
    C. NICE is designed to provide guidance on how to onboard new employees and delete accounts for departing personnel.
    D. NICE is designed to provide guidance on how to create cybersecurity programs to maintain compliance with regulations.

19. Posters are placed throughout the workplace reminding users to log off when leaving their workstations unattended. This is an example of which of the following programs?

    A. A security education program
    B. A security training program
    C. A security awareness program
    D. None of the above

20. A network engineer attends a one-week hands-on course on firewall configuration and maintenance. This is an example of which of the following programs?

    A. A security education program
    B. A security training program
    C. A security awareness program
    D. None of the above

21. The Board of Directors has a presentation on the latest trends in security management. This is an example of which of the following programs?

    A. A security education program
    B. A security training program

C. A security awareness program
D. None of the above

22. Companies have the legal right to perform which of the following activities?

A. Monitor user Internet access from the workplace
B. Place cameras in locker rooms where employees change clothes
C. Conduct a search of an employee's home
D. None of the above

23. Sanctions for policy violations should be included in which of the following documents?

A. The employee handbook
B. A confidentiality/nondisclosure agreement
C. An acceptable use agreement
D. All of the above

24. Studies often cite _____ as the weakest link in cybersecurity.

A. policies
B. people
C. technology
D. regulations

25. Which of the following is not a component of an Acceptable Use Agreement?

A. Handling standards
B. Sanctions for violations
C. Acknowledgment
D. Social media monitoring

26. Which of the following is a privacy regulation that has a goal to protect citizens' personal data and simplify the regulatory environment for international business by unifying the regulation within the European Union?

A. European Union General Data Protection Regulation (GDPR)
B. European Union PCI Council
C. European Union Gramm-Leach-Bliley Act (GLBA)
D. Privacy Data Protection of the European Union (PDPEU)

27. Which of the following regulations specifically stipulates that schools must have written permission to release any information from a student's education record?

    A. FERPA
    B. HIPAA
    C. DPPA
    D. FISMA

28. Best practices dictate that employment applications should *not* ask prospective employees to provide which of the following information?

    A. Last grade completed
    B. Current address
    C. Social security number
    D. Email address

29. After a new employee's retention period has expired, completed paper employment applications should be _____.

    A. cross-cut shredded
    B. recycled
    C. put in the trash
    D. stored indefinitely

30. Threat actors might find job posting information useful for which of the following attacks?

    A. A distributed denial of service attack (DDoS) attack
    B. A social engineering attack
    C. A man-in-the-middle attack
    D. An SQL injection attack

EXERCISES

EXERCISE 6.1: Analyzing Job Descriptions

1. Access an online job-posting service such as Monster.com.
2. Find two IT-related job postings.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following groups should be assigned responsibility for physical and environmental security?

   A. Facilities management
   B. Information security management
   C. Building security
   D. A team of experts including facilities, information security, and building security

2. Physical and environmental security control decisions should be driven by a(n) _____.

   A. educated guess
   B. industry survey
   C. risk assessment
   D. risk management

3. Which of the following terms best describes CPTED?

   A. Crime prevention through environmental design
   B. Crime prevention through environmental designation
   C. Criminal prevention through energy distribution
   D. Criminal prosecution through environmental design

4. The design of a secure site starts with the _____.

   A. natural surveillance
   B. territorial reinforcement
   C. natural access control
   D. location

5. Which of the following models is known as the construct that if an intruder can bypass one layer of controls, the next layer of controls should provide additional deterrence or detection capabilities?

   A. Layered defense model
   B. Perimeter defense model
   C. Physical defense model
   D. Security defense model

6. The mere fact that an area appears to be secure is in itself a _____.

   A. deterrent
   B. layer
   C. defense
   D. signature

7. Best practices dictate that data centers should be _____.

   A. well marked
   B. located in urban areas
   C. inconspicuous and unremarkable
   D. built on one level

8. Which of the following would be considered a "detection" control?

   A. Lighting
   B. Berms
   C. Motion sensors
   D. Bollards

9. Badging or an equivalent system at a secure facility should be used to identify _____.

   A. everyone who enters the building
   B. employees
   C. vendors
   D. visitors

10. Which of the following statements best describes the concept of shoulder surfing?

    A. Shoulder surfing is the use of a keylogger to capture data entry.
    B. Shoulder surfing is the act of looking over someone's shoulder to see what is on a computer screen.
    C. Shoulder surfing is the act of positioning one's shoulders to prevent fatigue.
    D. None of the above.

11. The term BYOD is used to refer to devices owned by _____.

    A. the company
    B. a vendor
    C. the employee
    D. a contractor

12. Which of the following statements is *not* true about data center best practices?

    A. Data center equipment must be protected from damage caused by power fluctuations or interruptions.
    B. Data center power protection devices must be tested on a scheduled basis for functionality and load capacity.
    C. Data center generators must be tested regularly according to manufacturer's instructions.
    D. You can optionally log all service and routine maintenance.

13. Which of the following terms best describes a prolonged increase in voltage?

    A. Power spike
    B. Power surge
    C. Power hit
    D. Power fault

14. Common causes of voltage variations include _____.

    A. lightning, storm damage, and electric demand
    B. using a power conditioner
    C. turning on and off computers
    D. using an uninterruptable power supply

15. Adhering to building and construction codes, using flame-retardant materials, and properly grounding equipment are examples of which of the following controls?

    A. Fire detection controls
    B. Fire containment controls
    C. Fire prevention controls
    D. Fire suppression controls

16. A Class C fire indicates the presence of which of the following items?

    A. Electrical equipment
    B. Flammable liquids
    C. Combustible materials
    D. Fire extinguishers

17. Confidential data can reside on which of the following items?

    A. Smartphones
    B. Cameras
    C. Scanners
    D. All of the above

18. Which of the following data types includes details about a file or document?

    A. Apparent data
    B. Hidden data
    C. Metadata
    D. Cache data

19. URL history, search history, form history, and download history are stored by the device _____.

    A. operating system
    B. browser
    C. BIOS
    D. ROMMON

20. Which of the following statements about formatting a drive is not true?

    A. Formatting a drive creates a bootable partition.
    B. Formatting a drive overwrites data.
    C. Formatting a drive fixes bad sectors.
    D. Formatting a drive permanently deletes files.

EXERCISES

EXERCISE 7.1: Researching Data Destruction Services

1. Research companies in your area that offer data destruction services.
2. Document the services they offer.
3. Make a list of questions you would ask them if you were tasked with selecting a vendor for data destruction services.