**Chapter 17 – Human Resources Security**

**TRUE/FALSE QUESTIONS:**

T F 1. Complying with regulations and contractual obligations is a benefit of

security awareness, training, and education programs.

T F 2. Employee behavior is not a critical concern in ensuring the security of

computer systems.

T F 3. Employees cannot be expected to follow policies and procedures of

which they are unaware.

T F 4. Security awareness, training, and education programs may be needed to

comply with regulations and contractual obligations.

T F 5. The education and experience learning level provides the foundation

for subsequent training by providing a universal baseline of key security terms and concepts.

T F 6. Security basics and literacy is required for those employees, including

contractor employees, who are involved in any way with IT systems.

T F 7. Awareness only communicates information security policies and

procedures that need to be followed and does not provide the foundation for any sanctions or disciplinary actions imposed for noncompliance.

T F 8. Awareness is used to explain the rules of behavior for using an

agency’s information systems and information and establishes a level of expectation on the acceptable use of the information and information systems.

T F 9. To emphasize the importance of security awareness, an organization

should have a security awareness policy document that is provided to all employees.

T F 10. Programmers, developers, and system maintainers require less

advanced security training than other employees.

T F 11. Security education is most often taught by outside sources.

T F 12. An employer cannot be held liable for negligent hiring if an

employee causes harm to a third party while acting as an employee.

T F 13. As part of their contractual obligation, employees should agree and

sign the terms and conditions of their employment contract, which should state their and the organization’s responsibilities for information security.

T F 14. Having all of the security functions and audit responsibilities reside in

the same person is a wise decision on the part of the organization.

T F 15. Many companies incorporate specific e-mail and Internet use policies

into the organization’s security policy document.

**MULTIPLE CHOICE QUESTIONS:**

1. \_\_\_\_\_\_\_ is a benefit of security awareness, training, and education programs to organizations.
2. Improving employee behavior
3. Increasing the ability to hold employees accountable for their actions
4. Mitigating liability of the organization for an employee’s behavior
5. All of the above
6. Security awareness, training, and education programs can serve as a deterrent to fraud and actions by disgruntled employees by increasing employees’ knowledge of their \_\_\_\_\_\_\_\_ and of potential penalties.

A. regulations B. accountability

C. liability D. incidents

1. The \_\_\_\_\_\_\_ category is a transitional stage between awareness and training.
2. roles and responsibilities relative to IT systems
3. security basics and literacy
4. education and experience
5. security awareness
6. \_\_\_\_\_\_\_\_ is explicitly required for all employees.
7. Security awareness
8. Education and experience
9. Security basics and literacy
10. Roles and responsibilities relative to IT systems
11. The \_\_\_\_\_\_\_\_\_ level focuses on developing the ability and vision to perform complex, multidisciplinary activities and the skills needed to further the IT security profession and to keep pace with threat and technology changes.
12. security basics and literacy
13. roles and responsibilities relative to IT systems
14. education and experience
15. security awareness
16. \_\_\_\_\_\_\_ are ways for an awareness program to promote the security message to employees.

A. Posters B. Newsletters

C. Workshops and training sessions D. All of the above

1. \_\_\_\_\_\_\_\_ need training on the development of risk management goals, means of measurement, and the need to lead by example in the area of security awareness.

A. Executives B. Analysts

C. Managers D. Trainers

8. From a security point of view, which of the following actions should be done upon the termination of an employee?

A. remove the person’s name from all lists of authorized access

B. recover all assets, including employee ID, disks, documents and equipment

C. remove all personal access codes

D. all of the above

9. \_\_\_\_\_\_\_\_ is the process of receiving, initial sorting, and prioritizing of information to facilitate its appropriate handling.

A. Incident B. Triage

C. Constituency D. Handling

10. CERT stands for \_\_\_\_\_\_\_\_\_\_\_.

A. Computer Error Response Team

B. Compliance Error Repair Technology

C. Computer Emergency Response Team

D. Compliance Emergency Response Technology

11. \_\_\_\_\_\_\_\_ can include computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.

A. Artifacts B. Vulnerabilities

C. CSIRT D. Constituencies

12. A capability set up for the purpose of assisting in responding to computer security-related incidents that involve sites within a defined constituency is called a \_\_\_\_\_\_.

A. CIRT B. CIRC

C. CSIRT D. all of the above

13. \_\_\_\_\_\_\_\_\_\_\_ scan critical system files, directories, and services to ensure they have not been changed without proper authorization.

A. Intrusion prevention systems

B. System integrity verification tools

C. Log analysis tools

D. Network and host intrusion detection systems

14. A \_\_\_\_\_\_\_ policy states that the company may access, monitor, intercept, block access, inspect, copy, disclose, use, destroy, or recover using computer forensics any data covered by this policy.

A. standard of conduct B. unlawful activity prohibited

C. company rights D. business use only

15. A \_\_\_\_\_\_\_ policy states that violation of this policy may result in immediate termination of employment or other discipline deemed appropriate by the company.

A. disciplinary action B. company rights

C. policy scope D. business use only

**SHORT ANSWER QUESTIONS:**

1. The principal problems associated with employee behavior are errors and omissions, \_\_\_\_\_\_\_, and actions by disgruntled employees.
2. There is a need for a continuum of learning programs that starts with \_\_\_\_\_\_\_, builds to training, and evolves into education.
3. The four layers of the learning continuum as summarized by NIST SP 800-16 are: security awareness, security basics and literacy, roles and responsibilities relative to IT systems, and the \_\_\_\_\_\_\_\_\_ level.
4. After security basics and literacy, training becomes focused on providing the knowledge, skills, and abilities specific to an individual’s \_\_\_\_\_\_\_ relative to IT systems.
5. In general, a(n) \_\_\_\_\_\_\_\_ program seeks to inform and focus an employee’s attention on issues related to security within the organization.
6. The principles that should be followed for personnel security are: limited reliance on key employees, separation of duties, and \_\_\_\_\_\_\_.
7. In large and medium-sized organizations, a(n) \_\_\_\_\_\_\_\_\_ is responsible for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.
8. Any action that threatens one or more of the classic security services of confidentiality, integrity, availability, accountability, authenticity, and reliability in a system constitutes a(n) \_\_\_\_\_\_\_\_.
9. \_\_\_\_\_\_\_\_ lists the following security objective with respect to current employees: “to ensure that employees, contractors, and third-party users are aware of information security threats and concerns and their responsibilities and liabilities with regard to information security and are equipped to support organizational security policy in the course of their normal work and to reduce the risk of human error”.
10. A(n) \_\_\_\_\_\_\_ is a characteristic of a piece of technology that can be exploited to perpetrate a security incident.
11. Network and host \_\_\_\_\_\_\_\_\_\_ monitor and analyze network and host activity and usually compare this information with a collection of attack signatures to identify potential security incidents.
12. The goal of the \_\_\_\_\_\_\_ function is to ensure that all information destined for the incident handling service is channeled through a single focal point regardless of the method by which it arrives for appropriate redistribution and handling within the service.
13. A(n) \_\_\_\_\_\_\_\_ is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures.
14. The group of users, sites, networks, or organizations served by the CSIRT is a(n) \_\_\_\_\_\_\_.
15. Employees have no expectation of \_\_\_\_\_\_ in their use of company-provided e-mail or Internet access, even if the communication is personal in nature.