

I. Security Management Practices Questions

1. Your company's security officer has requested that the IT department implement an authentication and authorization system based on biometrics. Which type of controls will you be implementing?
 - A) Administrative
 - B) Technical
 - C) Physical
 - D) Logical

2. What are the main 3 fundamental principles that a security program has as objectives?
 - A) Confidentiality, Integrity, Authenticity
 - B) Confusion, Ignorance, Annoyance
 - C) Confidentiality, Integrity, Availability
 - D) Security, Privacy, Authorization

3. A virus that shows up in the network environment and disrupts productivity is an example of which of the following?
 - A) Vulnerability
 - B) Threat
 - C) Risk
 - D) Exposure

4. Which of the following defines a countermeasure?
 - A) A procedure that can eliminate the threat.
 - B) A software configuration that can completely prevent a threat.
 - C) A software configuration, hardware, or procedure that can mitigate potential risk
 - D) Procedure that is done to fix the destruction that an exposure has caused.

5. When implementing a security program, which direction should be under taken by management for proper support and direction?
 - A) A top-down approach should be implemented, meaning that the implementation and support should come from the IT management and work its way down.
 - B) A bottom-up approach should be implemented, meaning that the implementation and support should come from the company top management and work its way up to the IT management and staff members.
 - C) A top-down approach should be implemented, meaning that the implementation and support should come from the company's top management and work its way through middle management and then to staff members.
 - D) A bottom-up approach should be under taken by the IT department developing a security program and implementing it in order to prove to proper management support and direction that is necessary.

6. The proper relation the words "threat", "exposure", and "risk" have to one another?
 - A) An "exposure" gives rise to a "threat" which exploits a "risk" and leads to a known vulnerability.
 - B) A "risk" causes a "vulnerability" that leads to a "threat" and causes an "exposure".
 - C) A "vulnerability" allows a "risk" that leads to a "threat" creating an "exposure".
 - D) A "threat" exploits a vulnerability that leads to a "risk", and can cause an "exposure".

7. Security models have many layers and different types of goals to accomplish in different time frames. Which of the following accurately describes the goals and their relationship?
- A) Tactical goals or daily goals, operational goals or mid term goals, strategic goals or long term goals. This approach to planning is called your planning horizon.
 - B) Strategic goals or long term goals, tactical goals or mid term goals, operational goals or daily goals, this approach to planning is called the Top-down approach.
 - C) Tactical goals or daily goals, operational goals or mid term goals, strategic goals or long term goals, this approach to planning is called your bottom-up approach.
 - D) Strategic goals or long term goals, tactical goals or mid term goals, operational goals or daily goals, this approach to planning is called your planning horizon.
8. You are trying to justify the security safeguards that you wish to implement. What would be your first step?
- A) Perform a threat analysis
 - B) Perform a risk analysis
 - C) Perform a top-down analysis
 - D) Perform a bottom-up analysis
9. To calculate the Annualized Loss Expectancy (ALE), which formula is used to calculate the financial loss to an organization for a threat?
- A) $SLE \times ARO$
 - B) $ALE \times (ARO - SLE)$
 - C) $AF \times EF$
 - D) $AF \times ARO$
10. According to specific studies dealing with loss to an organization through inappropriate network use, which group causes the most loss?
- A) Hackers
 - B) Network Intruders
 - C) Employees
 - D) Corporate Espionage
11. Organize the following government data classification from most sensitive to least sensitive.
(1) Confidential (2) Secret (3) Sensitive but Unclassified (SBU) (4) Unclassified (5) Top Secret
- A) 4, 3, 1, 2, 5
 - B) 5, 2, 1, 3, 4
 - C) 1, 2, 3, 5, 4
 - D) 5, 2, 3, 1, 4
12. Once you have established the risk and the cost of an organizational loss, you purchase insurance to reduce the risk. Which of the selections describe this act?
- A) Risk Assessment
 - B) Risk transfer
 - C) Risk rejecting
 - D) The game of Risk

13. Which one of the following describes the fundamental differences between procedures, guidelines, policies, and standards?
- A) A policy is the senior management statement that dictates what type of role that security plays. Procedures are a complete set of instructions designed to comply with mandatory standards and guidelines.
 - B) Procedures are managerial statements that dictate the policies for security and the standards and guidelines to be implemented.
 - C) Standards are the policies that senior management dictate to help formulate the procedures to implemented for security.
 - D) Standards are recommended guidelines. Procedures are directly implemented as a consequence of the security policy dictated by senior management.
14. Continual education of security awareness to the entire organization helps improve which of the following?
- A) The network will operate at an increased level and efficiency.
 - B) The network users will be able to detect another network user's abuses.
 - C) The IT staff will have the added knowledge of how to hack into its competitors' networks.
 - D) It aids the company's own view toward its security and protection of its systems and resources
15. Implementing security policies and the items that support them shows that a company is practicing which of the following?
- A) Due care
 - B) Due diligence
 - C) Risk prevention
 - D) Risk assessment
16. What is the main difference between the role of the Data Custodian and the Data Owner?
- A) The Data Custodian decides upon the classification of the data itself and delegates the day to day management of the data to the Data Owner
 - B) The Data Owner decides upon the classification of the data itself and delegates day to day management of the data to the Data Custodian
 - C) The Data Owner defines the classification of the data after the Data Custodian has secured the data.
 - D) The Data Custodian is usually a salaried employee working under the Data Owner.
17. Which of the following should be done upon the hiring of personnel?
- A) All personnel should sign the form 2163 according to HIPAA.
 - B) All personnel should be made to sign an NDA.
 - C) Coworkers should have the opportunity to perform interviews to confirm personality compatibility.
 - D) Extensive physical, emotional and psychological evaluations should be performed.

18. From least to most sensitive, order the following commercial data classifications.

(1) Private (2) Public (3) Confidential (4) Sensitive

- A) 2, 4, 1, 3
- B) 1, 2, 3, 4
- C) 4, 2, 1, 3
- D) 2, 1, 4, 3

19. What would be an appropriate difference between a qualitative and a quantitative risk analysis?

- A) Qualitative would be a subjective observation, while a quantitative approach defines statistical costs associated with a threat.
- B) Quantitative approach would be a subjective observation, while a qualitative approach defines statistical costs associated with a threat.
- C) Qualitative defines the overall appeal of a target or a resource, while quantitative is defined (threats x vulnerability x asset value) x controls gap.
- D) Quantitative approach indicates the total cost of the security implemented for protection, qualitative identifies the expected acceptance of the security policy from the organization.

20. Which of the following is not a characteristic of a Safeguard or countermeasure?

- A) Defaults to least privilege.
- B) Clear distinction between user and administrator.
- C) Must be testable.
- D) Removes the resource from accessibility as a response to an attack.

I. Security Management Practices Answers to Questions

1. The answer is B.
Technical: Biometric authentication systems fall under the category of Technical Controls. Technical controls are defined as logical access controls, encryption, security devices, and identification and authentication systems.
2. The answer is C.
CIA Triad – Confidentiality, Integrity and Availability. This is self-explanatory.
3. The answer is B.
Threat: A virus that shows up is a threat at this point. If we were calculating the possibility of a virus showing up, that would be a risk. If a virus showed up at your network and systems got infected, you would have an exposure. Not keeping the virus signatures up-to-date would be a vulnerability.
4. The answer is C.
Countermeasures can be any hardware, software, or procedure that helps to mitigate the potential risk.
5. The answer is C.
Top senior management should be the initiation of Security management within a corporation. Once buy-in from the top begins, then a successful top-down approach can begin.
6. The answer is D.
A threat can exploit a vulnerability, which leads to a risk that can damage an asset and causes an exposure, which can be counter-measured by a safeguard.
7. The answer is D.
In defining your planning horizon, you will need to define your strategic goals which are your long-term goals, your tactical goals or mid term goals, and your operational goals which are your daily goals.
8. The answer is B.
Performing a risk analysis will provide a means to justify the expense and countermeasures that must be implemented.
9. The answer is A.
The Annual Loss Expectancy (ALE) = Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO). The SLE is a calculation of the Asset value times its Exposure Factor. The Exposure factor is the percentage of damage an asset would incur in case of an occurrence. The ARO is the frequency such a threat poses.
10. The answer is C.
Employees are the most likely to cause damage to corporate systems. Many of the incidents go unreported or undocumented due to fear that it will cause a loss of confidence in the company from the public.

11. The answer is B.
Most sensitive to least sensitive for the following classifications would be: Top Secret, Secret, Confidential, Sensitive but unclassified, Unclassified.
12. The answer is B.
Purchasing insurance to help mitigate the risk of a threat is a means of transferring the risk to a third party making the risk that is left acceptable.
13. The answer is A.
Security policies are statements that originate from senior management. Standards are drawn up to provide uniform ways to carry out the desires of the Security policies. Guidelines are recommendation actions that are specific to ensure the standards. Procedures are detailed step-by-step actions to achieve the guidelines.
14. The answer is D.
The only answer that pertains to the company as a whole concerning security from an organizational view. The other answers are far too specific and are only a small part of security awareness.
15. The answer is B.
Due diligence is practiced by activities that make sure that the protection mechanisms are continually maintained and operational.
16. The answer is B.
The Data Owner is the one who decides upon the classification of the data. The Data Custodian is the one assigned by the owner to manage the data.
17. The answer is B.
The only one which pertains to a reasonable (and possible) employment request is the mandatory signing of an NDA.
18. The answer is A.
Commercial data classifications follow the order from least to most sensitive - Public, Sensitive, Private, Confidential.
19. The answer is A.
A quantitative approach is a calculation using statistics of odds and ratios about the possibilities of specific threats. A qualitative approach is more subjective using opinion polls and other subjective means that identify the priority of threats that poses possible risks.
20. The answer is D.
Removing a resource would make the resource unavailable. Thus violating one of the tenants of the CIA Triad. All the others are valid countermeasures.