Exam Report: 3.7.5 Practice Questions

Date: 1/16/2020 4:29:15 pm
Time Spent: 12:23

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 73%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

What is the primary purpose of forcing employees to take mandatory one-week minimum vacations every year?

- To check for evidence of fraud
- To prevent the buildup of significant vacation time
- To cut costs on travel
- To test their knowledge of security

Explanation

The primary purpose of requiring one-week mandatory vacations is to check for evidence of fraud in the worker's absence.

Prevention of the build-up of vacation time is not the purpose of the security principle of mandatory vacations; however some organizations perform this action for a monetary benefit. Mandatory vacations are not used to reduce travel costs or test employee security knowledge.

References

LabSim for Security Pro, Section 3.7.
[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_01||/]

Question 2: Correct

A code of ethics does all but which of the following?

- Clearly defines courses of action to take when a complex issue is encountered
- Serves as a reference for the creation of acceptable use policies
- Improves the professionalism of your organization as well as your profession
- Establishes a baseline for managing complex situations

Explanation

A code of ethics does not provide clear courses of action when faced with complex issues and situations. That's the whole problem with ethical dilemmas--a right or wrong answer is not always easily determined. A code of ethics describes best practices and helps steer intentions to allow individuals and organizations to respond to complex situations in the most appropriate manner.

A code of ethics does establish a baseline for managing complex situations, improves professionalism, and serves as a reference for the creation of acceptable use policies.

References

LabSim for Security Pro, Section 3.7.

[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_02]

Question 3: Correct

Which of the following are typically associated with human resource security policies? (Select two.)

- [ ] SLA
- [ ] Change management
- [x] Background checks
- [x] Termination
- [ ] Password policies

Explanation

Human resource policies related to security might include the following:

- Hiring policies, which identify processes to follow before hiring. For example, the policy might specify that pre-employment screening include a background check.
- Termination policies, which and procedures identify processes for terminating employees.
- A requirement for *job rotation*, which cross-trains individuals and rotates users between positions on a regular basis.
- A requirement for *mandatory vacations*, which requires employees to take vacations of specified length.

Service Level Agreements (SLAs), sometimes called maintenance contracts, guarantee the quality of a service to a subscriber by a network service provider. *Password policies* detail the requirements for passwords for the organization. A *change and configuration management policy* provides a structured approach to secure company assets and to make changes.

References

LabSim for Security Pro, Section 3.7.
[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_03]

Question 4: Correct

Which of the following is **not** part of security awareness training?

- ( ) Establish reporting procedures for suspected security violations
- ( ) Familiarize employees with the security policy
- (•) Employee agreement documents
- ( ) Communicate standards, procedures, and baselines that apply to the employee's job

Explanation

Employee agreement documents are part of employee management. The other options are all necessary parts of security awareness training.

References

LabSim for Security Pro, Section 3.7.
[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_04]

Question 5: Correct

Over the last month, you have noticed a significant increase in the occurrence of inappropriate activities performed by employees. What is the best first response step to take in order to improve or maintain the security level of the environment?

- (•) Improve and hold new awareness sessions
- ( ) Initiate stronger auditing
- ( )

Reduce all employee permissions and privileges

Terminate all offenders

Explanation

In this situation, the best response is to improve and hold new awareness sessions. If everyone is lax in avoiding inappropriate behavior, either they have forgotten what is appropriate, or a new trend has started that needs to be diverted. Either way, new awareness should greatly reduce occurrences.

Termination should only be considered after repeated attempts to re-train and warn the offenders. Firing staff based on initial trend data of inappropriate activities is an overly severe response. Reducing permissions and privileges is a step to take after re-training--otherwise, it could severely interfere with the ability of the staff to accomplish their work tasks. Initiating stronger auditing will not directly address the problem; it will just uncover more evidence of the trend of increasing inappropriate activity.

References

LabSim for Security Pro, Section 3.7.
[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_05]

Question 6: Incorrect

As you help a user with a computer problem, you notice that she has written her password on a note stuck to her computer monitor. You check the password policy of your company and find that the following settings are currently required:

- Minimum password length = 10
- Minimum password age = 4
- Maximum password age = 30
- Password history = 6
- Require complex passwords that include numbers and symbols
- Account lockout clipping level = 3

Which of the following is the best action to take to make remembering passwords easier so that she no longer has to write the password down?

Increase the maximum password age

Decrease the minimum password length

Increase the account lockout clipping level

~~Remove the complex password requirement~~

Implement end-user training

Explanation

The best solution is to implement end user training. Instruct users on the importance of security and teach them how to create and remember complex passwords. Making any other changes would violate the security policy and reduce the overall security of the passwords.

References

LabSim for Security Pro, Section 3.7.
[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_06]

Question 7: Correct

You have installed antivirus software on computers at your business. Within a few days, however, you notice that one computer has a virus. When you question the user, she says she installed some software a few days ago, but it was supposed to be a file compression utility. She admits she did not scan the file before running it.

What should you add to your security measures to help prevent this from happening again?

User awareness training

Close unused firewall ports

- Account lockout
- Proxy server

Explanation

Many antivirus prevention measures are ineffective if users take actions that put their computers at risk (such as downloading and running files or copying unscanned files to their computers). If users are educated about malware and about the dangers of downloading software, the overall security of the environment improves.

A proxy server controls access to the internet based on user name, URL, or other criteria. Account lockout helps prevent attackers from guessing passwords. Firewall ports might be used by some malware, but will not prevent malware introduced by downloading and installing a file.

References

LabSim for Security Pro, Section 3.7.
[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_07]

Question 8: Correct

Which of the following defines *two-man control*?

- An employee is granted the minimum privileges required to perform the position's duties.
- A situation in which multiple employees conspire to commit fraud or theft.
- Certain tasks should be dual-custody in nature to prevent a security breach.
- For any task in which vulnerabilities exist, steps within the tasks are assigned to different positions with different management.

Explanation

The principle of two-man control specifies that certain tasks should be dual-custody in nature to prevent a security breach.

The principle of least privilege specifies that an employee is granted the minimum privileges required to perform the position's duties. The principle of separation of duties specifies that for any task in which vulnerabilities exist, steps within the tasks are assigned to different positions with different management. Collusion is a situation in which multiple employees conspire to commit fraud or theft.

References

LabSim for Security Pro, Section 3.7.
[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_08]

Question 9: Correct

Which of the following is a legal contract between the organization and the employee that specifies the employee is not to disclose the organization's confidential information?

- Non-disclosure agreement
- Acceptable use agreement
- Non-compete agreement
- Employee monitoring agreement

Explanation

A non-disclosure agreement is a legal contract between the organization and the employee that specifies that the employee is not to disclose the organization's confidential information.

The non-compete agreement prohibits an employee from working for a competing organization for a specified time after the employee leaves the organization. The acceptable use agreement identifies the employee's rights to use company property, such as internet access and computer equipment, for personal use. The employee monitoring agreement outlines the organization's monitoring activities.

References

LabSim for Security Pro, Section 3.7.
[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_09]

Question 10: Correct

Your company security policy requires separation of duties for all network security matters. Which of the following scenarios best describes this concept?

- The system administrator configures remote access privileges and the security officer reviews and activates each account.
- Only the security officer can implement new border router rule sets.
- Security policy authors may never fraternize with system administration personnel.
- Every change to the default system image requires concurrent processing by multiple domain controllers.

Explanation

Separation of duties is designed to limit an individual's ability to cause severe damage or conduct unauthorized acts alone. By limiting the scope of authority and requiring multiple individuals to facilitate an action, exposure to malicious activity is greatly reduced. In this scenario, requiring the security officer to approve and activate all remote access requests is the best example of this concept.

References

LabSim for Security Pro, Section 3.7.
[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_10]

Question 11: Incorrect

Which of the following is **not** a protection against collusion?

- ~~Principle of least privilege~~
- Separation of duties
- Cross-training
- Two-man control

Explanation

Cross-training is not a protection against collusion because it trains each user to perform many job roles. This makes it possible for a single user to perform fraud and abuse or convince someone else to collude.

Separation of duties, two-man control, and principle of least privilege are all protections against collusion because they make it difficult for a single person to commit a crime by locking down privileges and access. Therefore, attempts to involve multiple people in such an environment are easily detected (in other words, these mechanisms serve as a prevention against collusion).

References

LabSim for Security Pro, Section 3.7.
[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_11]

Question 12: Correct

Which of the following is **not** an element of the termination process?

- Exit interview
- Disable all network access
- Dissolution of the NDA
- Return company property

Explanation

Employee termination does not dissolve the NDA (nondisclosure agreement). The exit interview should remind and re-enforce that the NDA is in effect even after their employment has ended.

Termination should trigger the disabling of all network access. In addition, all company property (such as keys, badges, phones, and computers) should be returned.

References

LabSim for Security Pro, Section 3.7.
[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_12]

Question 13: Correct

When you inform an employee that they are being terminated, what is the most important activity?

- Give them two week's notice
- Disable their network access
- Allow them to collect their personal items
- Allow them to complete their current work projects

Explanation

When an employee is terminated, their network access should be disabled immediately. Often, an employee is taken into an exit interview, where they are informed of the termination and asked to review their NDA and other security agreements. While the exit interview is occurring, the system administrator disables the user's network access and security codes.

Returning personal items is the least important task when removing an employee. Terminated employees should not be allowed to complete work projects, nor should they be given two week's notice. Both of these activities grant the ex-employee the ability to cause damage to your secure environment as a form of retaliation.

References

LabSim for Security Pro, Section 3.7.
[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_13]

Question 14: Incorrect

The best way to initiate solid administrative control over an organization's employees is to have what element in place?

- ~~Rotation of duties~~
- An acceptable use policy
- Mandatory vacations in one-week increments
- Distinct job descriptions

Explanation

Distinct job descriptions are the foundation of solid administrative control. With written job descriptions, all security needs for each employee are defined and prescribed.

An acceptable use policy is important, but it is nearly useless unless it clearly defines what employees should do and what employees will be held responsible for based upon the employee's position. Rotation of duties is only possible if there are distinct job descriptions. Mandatory vacations are only effective if distinct job descriptions exist to define what is to be reviewed and audited in the employee's absence.

References

LabSim for Security Pro, Section 3.7.
[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_14||/]

Question 15: Incorrect

Match the employment process on the left with the task that should occur during each process on the right.

Each process may be used once, more than once, or not at all.

Conduct role-based training

✔ Employment

Verify an individual's job history

✔ Pre-employment

Show individuals how to protect sensitive information

✔ Employment

Disable a user's account

✔ Termination

Remind individuals of NDA agreements

~~Employment~~ Termination

Obtain an individual's credit history

✔ Pre-employment

Explanation

During the pre-employment process, you need to determine whether an individual is a valid security risk by performing tasks such as the following:

- Verify the prospective employee's job history
- Obtain a credit history (if appropriate)

During the employment phase, you need to ensure employees are made aware of security issues. Some of the measures you can implement include the following:

- Make employees aware of the standards, procedures, and baselines that apply to the employee's specific job. This is referred to as *role-based training*.
- Make employees aware of what constitutes sensitive information and steps that should be taken to protect it.

The termination process identifies the tasks an organization takes when an employee voluntarily or involuntarily leaves the organization. Be sure to complete the following:

- Remind the employee of any agreements related to non-disclosure and non-compete.
- Disable the employee's accounts, including physical access, electronic access, and telephone access.

References

LabSim for Security Pro, Section 3.7.
[All Questions SecPro2017_v6.exm EMPLOYEE_MGMT_15]