Exam Report: 3.2.4 Practice Questions

Date: 1/14/2020 1:53:48 pm
Time Spent: 8:58

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 73%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following is **not** an appropriate response to a risk discovered during a risk analysis?

- Denial
- ~~Mitigation~~
- Assignment
- Acceptance

Explanation

Denial or ignoring risk is not an appropriate response. Denying risk rather than properly addressing it is a negligent activity that can be used against an organization in court if a security breach occurs that causes damages affecting investors or the public.

Valid responses to risk are acceptance, assignment, and mitigation.

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_02]

Question 2: Correct

Which of the following best defines Single Loss Expectancy (SLE)?

- The monetary value of a single employee's loss of productivity due to a successful attack
- The total cost of all countermeasures associated with protecting against a given vulnerability
- The statistical probability of a malicious event
- The total monetary loss associated with a single occurrence of a threat

Explanation

Single Loss Expectancy (SLE) is best defined as the total monetary loss associated with a single occurrence of a threat. The key to this definition is 'total'- all costs, including lost employee productivity, replacement hardware/software, payroll for additional consultants, etc., must be considered when calculating the total loss.

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_03]

Question 3: Correct

What is the average number of times that a specific risk is likely to be realized in a single year?

- Exposure factor
- Annualized rate of occurrence
- Estimated maximum downtime
- Annualized loss expectancy

Explanation

Annualized Rate of Occurrence (ARO) is the average number of times that a specific risk is likely to be realized in a single year.

Annualized Loss Expectancy (ALE) is ARO x SLE (Single Loss Expectancy), which is the estimated per-year loss due to exposures. Estimated Maximum Downtime sounds similar to maximum tolerable downtime or recovery time objective, neither of which are related to the average number of times of risk realization. Exposure factor is the percentage of value loss that is experienced due to an exposure, rather than the number of times of exposure.

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_04]

Question 4: Correct

Your company has developed and implemented countermeasures for the greatest risks to their assets. However, there is still some risk left. What is the remaining risk called?

- Residual risk
- Exposure
- Loss
- Risk

Explanation

Residual risk is the portion of risk that remains after the implementation of a countermeasure. There will almost always be some residual risk.

Exposure is the vulnerability of losses from a threat agent. *Risk* is the likelihood of a vulnerability being exploited. A *loss* is the real damages to an asset that reduces its confidentiality, integrity, or availability.

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_05]

Question 5: Correct

Which of the following statements is true regarding risk analysis? (Select two.)

- [x] Don't implement a countermeasure if the cost is greater than loss.
- [ ] The value of an asset is the worth of a resource to the organization excluding qualitative values.
- [x] Annualized Rate of Occurrence (ARO) identifies how often the successful threat attack will occur in a single year.
- [ ] Exposure factor is the percent of the asset lost from an unsuccessful threat attack.

Explanation

The cost of a countermeasure should never exceed the value of the asset. Annualized Rate of Occurrence (ARO) identifies how often the successful threat attack will occur in a single year.

The *value* of an asset is the worth of a resource to the organization, including *both* quantitative and qualitative values. *Exposure factor* is the percent of the asset lost from a *successful* threat attack.

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_07]

Question 6: Correct

When would choosing to do nothing about an identified risk be acceptable?

- When the asset is an intangible asset instead of a tangible asset
- When the threat is likely to occur less than once per year
- When the cost of protecting the asset is greater than the potential loss
- When the threat is most likely to come from an internal source instead of an external source

Explanation

You might choose to accept a risk and do nothing if the cost associated with a threat is acceptable or if the cost of protecting the asset from the threat is unacceptable. For example, if the cost of protecting the asset is greater than the cost associated with the threat, you would decide to accept the potential loss rather than spend money to protect the asset. In this case, you would plan for how to recover from the threat, but not implement any measures to avoid it.

An *intangible asset* is a resource that has value and may be saleable even though it is not physical or material. While assigning a value to intangible assets can be difficult, this does not mean that they cannot or should not be protected. The likely frequency of a threat occurring affects the annual loss expectancy, which also affects the comparison of the cost of countermeasures to the cost associated with a successful attack, but does not immediately rule out implementing countermeasures.

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_08]

Question 7: Correct

If an organization shows sufficient due care, which burden is eliminated in the event of a security breach?

- Liability
- Negligence
- Investigation
- Asset loss

Explanation

An organization with sufficient due care has shown that they have taken every reasonable effort to protect their assets and environment. If a security breach occurs, then the organization is not held negligent for the losses.

Even with a strong security solution, asset loss is always possible. Even with strong due care, an organization is still liable for damages incurred. Due care does not remove the requirement to investigate security breaches.

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_09]

Question 8: Incorrect

You have conducted a risk analysis to protect a key company asset. You identify the following values:

- Asset value = 400
- Exposure factor = 75
- Annualized rate of occurrence = .25

What is the Annualized Loss Expectancy (ALE)?

- 25
- 75
- ~~100~~
- 175
- 475

Explanation

To calculate the ALE, use the following formula:

Asset value (AV) x exposure factor (EF) x Annualized Rate of Occurrence (ARO)
400 x 75% x .25 = 75

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_10]

Question 9: Incorrect

When conducting a risk assessment, how is the Annualized Rate of Occurrence (ARO) calculated?

- Divide the static variable by the probability index.
- ~~Multiply the Single Loss Expectancy (SLE) by the Annual Loss Expectancy (ALE).~~
- Through historical data provided by insurance companies and crime statistics.
- Multiply the Single Loss Expectancy (SLE) by the standard annual deviation.

Explanation

The Annualized Rate of Occurrence (ARO) is the likelihood of a risk occurring within one year. Historical data provides the basis for the statistical probability of the risk occurring. This information is frequently obtained from insurance companies, law enforcement agencies, and computer incident monitoring organizations. ARO is typically expressed in percent or decimal form.

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_11]

Question 10: Correct

Purchasing insurance is what type of response to risk?

- Transference
- Acceptance
- Rejection
- Deployment of a countermeasure

Explanation

An organization can *transfer* risk through the purchase of insurance. When calculating the cost of insurance and the deductible, balance the cost against the expected loss from the incident.

Risk *acceptance* is the decision that the level of risk is acceptable. Risk *rejection* is choosing not to respond to the risk even though the risk is not at an acceptable level. The deployment of countermeasures entails choosing and putting into practice those countermeasures that reduce the risk to an acceptable level.

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_12]

Question 11: Correct

To determine the value of the company assets, an anonymous survey was used to collect the opinions of all senior and mid-level managers. Which asset valuation method was used?

- Sensitivity vs. risk
- Delphi method
- Asset classification
- Comparative

Explanation

The *delphi method* uses an anonymous survey to determine the value of an asset. Anonymity promotes honesty in responses.

Asset *classification* is used to identify the appropriate value and protection levels for each asset. A *comparative* valuation uses a ranking based on an arbitrary scale that is compatible with the organization's industry. A *sensitivity vs. risk* chart uses quadrants to qualify the value of an asset based on sensitivity and risk.

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_13]

Question 12: Incorrect

You have conducted a risk analysis to protect a key company asset. You identify the following values:

- Asset value = 400
- Exposure factor = 75
- Annualized Rate of Occurrence = .25

What is the Single Loss Expectancy (SLE)?

- ~~100~~
- 300
- 475
- 30000

Explanation

The Single Loss Expectancy (SLE) is the asset value (AV) multiplied by the exposure factor (EF), with the EF being a percentage of the asset value that is lost. In this example, SLE = 400 x 75% = 300.

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_14]

Question 13: Correct

A broken water pipe that floods the reception area would be considered which type of threat?

- Disaster
- Internal
- External
- Natural

Explanation

Natural events are those events that may reasonably be expected to occur over time. Examples are a fire or a broken water pipe.

Disasters are major events that have significant impact on an organization. Examples are tornadoes, hurricanes, and floods.

External threats are those events originating outside of the organization that typically focus on compromising the organization's information assets.

Internal threats are intentional or accidental acts by employees. Examples are theft, fraud, snooping, and unintentional data loss.

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_16||/]

Question 14: Correct

A file server with data is consider which of the following asset types?

- Intangible
- Tangible
- Neither tangible nor intangible
- Both tangible and intangible

Explanation

Assets can have both tangible and intangible components. For example, a computer that functions as a server has a tangible value associated with the replacement cost of the hardware. Intangible assets include the data on the computer, the value of the role that the computer performs within the organization, and what the computer's information is worth to a competitor or an attacker.

A tangible asset is a physical item such as a computer, storage device, or document. Such items are typically purchased.

An intangible asset is a resource that has value and may be saleable even though it is not physical or material. Intangible assets are typically more challenging to identify and evaluate.

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_17||/]

Question 15: Correct

Which of the following is **not** an accepted countermeasure to strengthen a cryptosystem?

- Keep the cryptosystem a secret
- Implement long key spaces
- Use strong passwords
- Implement strong systems with redundant encipherment

Explanation

Current practice in cryptography does not rely on the secrecy of the cryptosystem. Publishing the algorithm exposes the system to scrutiny. This scrutiny often validates the security of the system or identifies weaknesses that show the system as unreliable.

The following countermeasures can strengthen a cryptosystem:

- Use strong passwords that contain multiple character types, are a minimum length of eight characters or more, and use no part of a username or email address.
- Implement strong cryptosystems with redundant encipherment, such as 3DES.

• Implement long key spaces. Generally speaking, the longer the key space, the stronger the cryptosystem.

References

LabSim for Security Pro, Section 3.2.
[All Questions SecPro2017_v6.exm RISK_MANAGE_01]