Exam Report: 12.2.6 Practice Questions

Date: 11/20/2019 5:42:55 pm
Time Spent: 6:45

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 36%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following is an example of an internal threat?

- A user accidentally deletes the new product designs.
- ~~A delivery man is able to walk into a controlled area and steal a laptop.~~
- A water pipe in the server room breaks.
- A server backdoor allows an attacker on the internet to gain access to the intranet site.

Explanation

Internal threats are intentional or accidental acts by employees, including:

- Malicious acts such as theft, fraud, or sabotage.
- Intentional or unintentional actions that destroy or alter data.
- Disclosing sensitive information through snooping or espionage.

External threats are the events originating outside of the organization that typically focus on compromising the organization's information assets. Examples are hackers, fraud perpetrators, and viruses. Natural events are the events that may reasonably be expected to occur over time. Examples are a fire or a broken water pipe.

References

LabSim for Network Pro, Section 12.2.
[netpro18v5_all_questions_en.exm SP08_4-1 1]

Question 2: Incorrect

What is the greatest threat to theft of data in most secure organizations?

- USB devices
- Hacker intrusion
- Malware
- ~~Operator error~~

Explanation

The greatest threat to the confidentiality of data in most secure organizations is portable devices (including USB devices). There are so many devices that can support file storage that stealing data has become easy, and preventing data is very difficult.

References

LabSim for Network Pro, Section 12.2.
[netpro18v5_all_questions_en.exm CISSP-1020 [7]]

Question 3: Incorrect

Which of the following network strategies connects multiple servers together so that if one server fails, the others immediately take over its tasks, preventing a disruption in service?

- Storage area networks (SANs)
- Adapter bonding
- ~~Mirroring~~
- Clustering

Explanation

Clustering connects multiple servers together using special software. If one of the servers in the cluster fails, the other servers immediately take over the tasks the failed server was working on, resulting in no downtime for the end user.

Adapter bonding increases the fault tolerance of a single server system by implementing multiple network boards that function as a single adapter. Mirroring also increases fault tolerance by creating a mirror copy of the server hard drive on one or more other hard drives. Storage area networks are usually used in conjunction with clustering to provide a common disk system that all servers in the cluster share.

References

LabSim for Network Pro, Section 12.2.
[netpro18v5_all_questions_en.exm SRVP_1-13 [33]]

Question 4: Incorrect

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

- Investigation
- ~~Liability~~
- Asset loss
- Negligence

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 requirement to investigate security breaches.

References

LabSim for Network Pro, Section 12.2.
[netpro18v5_all_questions_en.exm SP02_5-4 [13]]

Question 5: Incorrect

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 countermeasures that reduce the risk to an acceptable level.

References

LabSim for Network Pro, Section 12.2.
[netpro18v5_all_questions_en.exm SSCP-6 NEW [105]]

Question 6: 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?

Exposure

Loss

Risk

Residual risk

Explanation

Residual risk is the portion of risk that remains after a countermeasure is implemented. 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 Network Pro, Section 12.2.
[netpro18v5_all_questions_en.exm SSCP-6 NEW [97]]

Question 7: Correct

When is choosing to do nothing about an identified risk acceptable?

When the threat is most likely to come from an internal source instead of an external source.

When the asset is an intangible asset instead of a tangible asset.

When the cost of protecting the asset is greater than the potential loss.

When the threat is likely to occur less than once a year.

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 will also affect 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 Network Pro, Section 12.2.
[netpro18v5_all_questions_en.exm SP08_4-1 2]

Question 8: Incorrect

What is the primary goal of business continuity planning?

- ~~Minimizing the risk of delays and interruptions in services~~
- Maintaining business operations with reduced or restricted infrastructure capabilities or resources
- Minimizing decision-making during the development process
- Protecting an organization from major computer services failure

Explanation

The primary goal of BCP is maintaining business operations with reduced or restricted infrastructure capabilities or resources.

Minimizing the risk to the organization from delays and interruptions in providing services is a goal of DRP. If your organization cannot provide services, it is experiencing a disaster. Minimizing decision-making during the development process is not a valid goal of BCP or DRP; decisions should be made during development. The correct DRP goal is to minimize decisions during an emergency. Protecting an organization from major computer services failure is a goal of DRP, not BCP. If computer services fail, business continuity is interrupted, which is considered a disaster.

References

LabSim for Network Pro, Section 12.2.
[netpro18v5_all_questions_en.exm SSCP-6 CP [252]]

Question 9: Incorrect

In business continuity planning, what is the primary focus of the scope?

- ~~Human life and safety~~
- Company assets
- Business processes
- Recovery time objective

Explanation

Business processes are the primary focus of the scope of BCP.

Company assets are the focus of risk assessment for security policy development, not BCP. Human life and safety are considerations for emergency response, but are not the focus of the BCP scope. Recovery time objective is a consideration in the development of emergency response, not an aspect of BCP scope.

References

LabSim for Network Pro, Section 12.2.
[netpro18v5_all_questions_en.exm SSCP-7 CP [198]]

Question 10: Incorrect

When analyzing assets, which analysis method assigns financial values to assets?

- ~~Qualitative~~
- Transfer
- Quantitative
- Acceptance

Explanation

Quantitative analysis assigns a financial value, or a real number, and the cost required to recover from a loss to each asset.

Qualitative analysis seeks to identify costs that cannot be concretely defined using quantitative analysis. Transfer and acceptance are responses to risk, not risk analysis methods.

References

LabSim for Network Pro, Section 12.2.
[netpro18v5_all_questions_en.exm SSCP-6 NEW [113]]

Question 11: Correct

You manage the website for your company. The Web1 server hosts the website. This server has the following configuration:

- Dual core processor
- Dual power supplies
- RAID 5 volume
- One RAID controller
- Two 1000 Mbps network adapters

Which component is a single point of failure for the website?

- Disk storage
- Disk controller
- Power supply
- Network adapter

Explanation

A single point of failure means that failure in one component will cause the entire website to be unavailable. In this scenario, the disk controller is a single point of failure. If the disk controller fails, content for the website will be unavailable.

To prevent a single point of failure, provide redundant components. Dual power supplies, multiple network connections, and fault tolerant volumes (RAID 1, RAID 5, or RAID 0 + 1) can all sustain a failure in one component and continue to function.

References

LabSim for Network Pro, Section 12.2.
[netpro18v5_all_questions_en.exm SP08_6-1 2]

Question 12: Correct

You manage a website for your company. The website uses three servers configured in a cluster. Incoming requests are distributed automatically between the three servers. All servers use a

shared storage device that holds the website contents. Each server has a single network connection and a single power supply.
Considering the availability of your website, which component represents a single point of failure?

- Web server
- Power supply
- Network adapter
- ➡ Website storage

Explanation

In this scenario, the shared storage is a single point of failure. A single point of failure means that failure in one component will cause the entire website to become unavailable. If the storage unit fails, then the website content will be unavailable.

Failure in a single network card, power supply, or even in a single server will not make the website unavailable. Any of these failures will take one server offline. But because of the server cluster, other servers will still be available to process incoming requests.

References

LabSim for Network Pro, Section 12.2.
[netpro18v5_all_questions_en.exm SP08_6-1 1]

Question 13: Incorrect

When recovery is being performed due to a disaster, which services are to be stabilized first?

- ~~Outside communications~~
- Least business critical
- ➡ Mission critical
- Financial support

Explanation

Restore mission critical services first. If mission critical services are not restored within their maximum tolerable downtime, the organization is no longer viable.

Restore the least critical services last. Financial support and outside communications are restored only after all other services with a higher level of criticality have been restored.

References

LabSim for Network Pro, Section 12.2.
[netpro18v5_all_questions_en.exm CISSP-803 NEW [71]]

Question 14: Correct

Which of the following is not a valid response to a risk discovered during a risk analysis?

- Mitigation
- ➡ Denial
- Assignment
- Acceptance

Explanation

Denial, or ignoring risk, is not a valid response. Denying risk rather than properly addressing

risk is a negligent activity that can be used against an organization in court if a security breach occurs that damages investors or the public.

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

References

LabSim for Network Pro, Section 12.2.
[netpro18v5_all_questions_en.exm SP02_5-7 [37]]