Chp 13 NS

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/22/2022 1:50:05 pm • Time spent: 01:55

Score: 95%

Passing Score: 80%

Question 1: ✓ Correct

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

13.2.4 Analyzing Risks Facts

q_anylz_risk_ale_02_secp7.question.fex

Question 2: ✓ Correct

When should a hardware device be replaced in order to minimize downtime?

- ○ When its performance drops below 75% efficiency
- ○ Once every year
- ➡ ● Just before its MTBF is reached
- ○ Only after its first failure

EXPLANATION

Hardware should be replaced just before its MTBF (mean time between failures) is reached. This is the statistical average time that the device operates before experiencing its first serious failure.

Once every year is not an appropriate replacement metric, as many devices have an MTBF of 3 to 10 years or more. Waiting until a device experiences a failure does not minimize downtime. Instead, that is a scheme to minimize hardware costs by using every device until failure before replacement. Waiting for a performance efficiency drop is an ineffective solution, as most hardware failures do not provide such pre-failure symptoms.

REFERENCES

13.2.6 Business Continuity Planning Facts

q_biz_cont_mtbf_secp7.question.fex

Question 3: ✓ Correct

Change control should be used to oversee and manage changes over which aspect of an organization?

○ IT hardware and software

○ Personnel and policies

○ Physical environment

➡ ● Every aspect

EXPLANATION

Every aspect of an organization should be monitored and managed by change control.

Focusing only on hardware and software, personnel and policies, or the physical environment limits the effectiveness of change control. Change control should cover the entire organization.

REFERENCES

13.1.8 Credential and Organizational Policies Facts

q_cred_org_pol_change_04_secp7.question.fex

Question 4: ✓ Correct

Which of the following BEST describes an email security gateway?

- ○ It accepts mail and forwards it to other mail servers.
- ○ It provides a form of identity verification.
- ➡ ● It monitors emails that originate from an organization.
- ○ It requires the use of a public key certificate.

EXPLANATION

An email security gateway is a security solution that monitors emails that are sent to or originate from an organization.

Email encryption digitally signs an email with a certificate. The certificate provides a form of identity verification.

The important thing to understand about Secure/Multipurpose Internet Mail Extensions (S/MIME) is that it requires the use of a public key certificate in order to encrypt and decrypt email messages.

An SMTP relay is an email server that accepts mail and forwards it to other mail servers.

REFERENCES

13.3.2 Email Security Facts

q_email_sec_gateway_secp7.question.fex

Question 5: ✓ Correct

Which of the following is defined as a contract that prescribes the technical support or business parameters a provider bestows to its client?

- ➡ ● Service level agreement
- ○ Certificate practice statement
- ○ Final audit report
- ○ Mutual aid agreement

EXPLANATION

A service level agreement is defined as a contract that prescribes the technical support or business parameters a provider bestows to its client.

A mutual aid agreement is an agreement between two organizations to support each other in the event of a disaster. A final audit report is the result of an external auditor's inspection and analysis of an organization's security status. A certificate practice statement defines the actions and promises of a certificate service authority.

REFERENCES

13.1.4 Managing Third Parties Facts

q_man_thirdparties_sla_01_secp7.question.fex

Question 6: ✓ 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 monetary loss associated with a single occurrence of a threat.
- ○ The total cost of all countermeasures associated with protecting against a given vulnerability.
- ○ The statistical probability of a malicious event.

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 the term total. In other words, this encompasses all costs, including lost employee productivity, replacement hardware/software, and payroll for additional consultants. All of this must be considered when calculating the total loss.

REFERENCES

13.2.4 Analyzing Risks Facts

q_anylz_risk_sle_01_secp7.question.fex

Question 7: ✓ Correct

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

➡ ● Both tangible and intangible

○ Intangible

○ Tangible

○ Neither tangible nor 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

13.2.6 Business Continuity Planning Facts

q_biz_cont_asset_secp7.question.fex

Question 8: ✓ Correct

In a high-security environment, which of the following is the most important concern when removable media is no longer needed?

➡ ● Destruction

○ Reuse

○ Purging

○ Labeling

EXPLANATION

The most important concern is the destruction of the media. In a high-security environment, removable media is not reused. After the media is no longer needed, it must be destroyed.

Labeling is important, but it is important before removable media is put into use, not after. Reuse and purging are not secure activities in a high-security environment. Reusing media can result in confidentiality compromise. Purging is rarely sufficient to fully remove data.

REFERENCES

13.1.6 Data Protection and Policies Facts

q_dataprot_pol_retention_secp7.question.fex

Question 9: ✓ Correct

Which of the following BEST describes phishing?

➡ ● A fraudulent email that claims to be from a trusted organization.

○ An email server that accepts mail and forwards it to other mail servers.

○ Malware that often uses email as its distribution mechanism.

○ Unwanted and unsolicited email sent to many recipients.

EXPLANATION

Phishing is a fraudulent email that claims to be from a trusted organization.

Spam is unwanted and unsolicited email sent to many recipients.

A virus is malware that often uses email as its distribution mechanism.

An SMTP relay is an email server that accepts mail and forwards it to other mail servers.

REFERENCES

1.2.3 Defense Planning Facts

2.3.1 Social Engineering Overview

2.3.2 Social Engineering Overview Facts

2.3.3 Social Engineering Motivation

2.3.4 Social Engineering Motivation Facts

2.3.5 Social Engineering Techniques

2.3.6 Social Engineering Techniques Facts

2.3.7 Phishing and Internet-Based Techniques

2.3.8 Phishing and Internet-Based Techniques Facts

2.3.9 Use the Social Engineer Toolkit

2.3.10 Investigating a Social Engineering Attack

2.3.11 Identify Social Engineering

5.6.4 Web Threat Protection Facts

13.3.2 Email Security Facts

q_email_sec_phishing_02_secp7.question.fex

Question 10: ✓ Correct

How often should change-control management be implemented?

- ○ At regular intervals throughout the year.
- ○ Only when changes are made that affect senior management.
- ➡ ● Any time a production system is altered.
- ○ Only when a production system is altered greatly.

EXPLANATION

Management of change control is necessary any time a production system is altered.

REFERENCES

13.1.8 Credential and Organizational Policies Facts

q_cred_org_pol_change_01_secp7.question.fex

Question 11: ✓ Correct

Your company is preparing to enter into a partner relationship with another organization. It will be necessary for the information systems used by each organization to connect and integrate with each other.

Which of the following is of primary importance as you take steps to enter into this partner relationship?

- ○ Identify how data ownership is to be determined
- ○ Ensure that both organizations have similar incident-response procedures
- ➡ ● Ensure that the integration process maintains the security of each organization's network
- ○ Ensure that all aspects of the relationship are agreed upon in writing

EXPLANATION

The most important step to take as the two parties enter into this partner relationship is to ensure that the integration process maintains the security of each organization's network.

Identifying how data ownership is to be determined, ensuring that all aspects of the relationship are agreed upon in writing, and finding out if both organizations have similar incident-response procedures are steps that make sure that the security of each organization's network is maintained.

REFERENCES

13.1.2 Personnel Policy Facts

q_pers_pol_partner_secp7.question.fex

Question 12: ✓ Correct

What is a service level agreement (SLA)?

➡ ● A guarantee of a specific level of service.

○ An agreement to support another company in the event of a disaster.

○ A contract with a legal entity to limit your asset-loss liability.

○ A contract with an ISP for a specific level of bandwidth.

EXPLANATION

An SLA is a guarantee of a specific level of service from a vendor. That service may be communication links, hardware, or operational services. An SLA is a form of insurance against disasters or security intrusions that may affect your organization's mission-critical business functions.

An agreement to support another company in the event of a disaster is known as a mutual aid agreement. A contract with a legal entity to limit your asset-loss liability is an insurance policy. A contract with an ISP for a specific level of bandwidth is a service contract.

REFERENCES

13.1.4 Managing Third Parties Facts

q_man_thirdparties_sla_02_secp7.question.fex

Question 13: ✓ Correct

You have been receiving a lot of phishing emails sent from the domain kenyan.msn.pl. Links within these emails open new browser windows at youneedit.com.pl.

You want to make sure that these emails never reach your inbox, but you also want to make sure that emails from other senders are not affected.

What should you do?

- ➡ ● Add **kenyan.msn.pl** to the email blacklist.
- ○ Add **pl** to the email blacklist.
- ○ Add **youneedit.com.pl** to the email blacklist.
- ○ Add **msn.pl** to the email blacklist.

EXPLANATION

Add **kenyan.msn.pl** to the email blacklist. Adding **msn.pl** or **pl** to the blacklist filters out all emails from kenyan.msn.pl, but this also filters out other emails from the msn.pl or pl domains. Adding **youneedit.com.pl** to the email blacklist would prevent emails from that domain, but it would not prevent emails from kenyan.msn.pl, nor would it prevent links in the emails from opening windows to youneedit.com.pl.

REFERENCES

13.3.2 Email Security Facts

q_email_sec_blacklist_secp7.question.fex

Question 14: ✓ Correct

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

- ➡ ● Quantitative
- ○ Acceptance
- ○ Transfer
- ○ Qualitative

EXPLANATION

Quantitative analysis assigns a financial value or assignment of real numbers and the cost required to recover from a loss to the asset.

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

REFERENCES

☰ 13.2.4 Analyzing Risks Facts

q_anylz_risk_quantitative_secp7.question.fex

Question 15: ✓ Correct

Which of the following terms describes the actual time required to successfully recover operations in the event of an incident?

- ➡ ● Recovery time objective (RTO)
- ○ Maximum tolerable downtime (MTD)
- ○ Mean time to repair (MTTR)
- ○ Recovery point objective (RPO)

EXPLANATION

Recovery time objective (RTO) is the actual time required to successfully recover all operations.

The mean time to repair (MTTR) is an indication of how long it would typically take to get the system back online. Recovery point objective (RPO) is a measurement of how old data is at the point that it is successfully recovered. Any data that has been lost between the RPO and the present must either be accepted as lost or reconstructed. Maximum tolerable downtime (MTD) identifies the length of time an organization can survive with a specified service, asset, or process down.

REFERENCES

13.2.6 Business Continuity Planning Facts

q_biz_cont_rto_secp7.question.fex

Question 16: ✓ Correct

When you inform an employee that he or she is being terminated, which of the following is the most important activity?

➡ ● Disable his or her network access

○ Give him or her two weeks' notice

○ Allow him or her to collect their personal items

○ Allow him or her to complete their current work projects

EXPLANATION

When an employee is terminated, you should disable his or her network access 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 should disable 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 weeks' notice. Both of these activities grant the ex-employee the ability to cause damage to your secure environment as a form of retaliation.

REFERENCES

13.1.4 Managing Third Parties Facts

q_man_thirdparties_offboarding_secp7.question.fex

Question 17: ✓ Correct

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

○ External

➡ ● Natural

○ Internal

○ Disaster

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

13.2.6 Business Continuity Planning Facts

q_biz_cont_environ_secp7.question.fex

Question 18: ✕ Incorrect

Which of the following mechanisms can you use to add encryption to email? (Select two.)

- ☑ ~~Secure Shell~~
- ➡ ☐ S/MIME
- ☐ HTTPS
- ☐ Reverse DNS
- ➡ ☑ PGP

EXPLANATION

Use Pretty Good Privacy (PGP) or Secure MIME (S/MIME) to add encryption to emails.

HTTPS is used by web browsers to request data from web servers. Secure Shell (SSH) is a secure remote management utility. Reverse DNS can be used to verify the sending device's IP address included in an email. However, this does not add encryption to email messages.

REFERENCES

13.3.2 Email Security Facts

q_email_sec_smime_secp7.question.fex

Question 19: ✓ Correct

If an SMTP server is not properly and securely configured, it can be hijacked and used maliciously as an SMTP relay agent. Which activity could result if this happens?

○ Data diddling

○ Salami attack

➡ ● Spamming

○ Virus hoax

EXPLANATION

Attackers often distribute spam by hijacking a misconfigured SMTP server. SMTP servers that act as relay agents for unauthorized or external users can be easily employed to deliver spam. It is extremely important to properly configure SMTP servers to accept email only from authorized internal users.

A salami attack is an attack where small amounts of information, data, or valuables are taken over a period of time. The result is to construct or obtain data or property of great value. A common example of a salami attack is to deposit the fractions of cents from an accounting program into a numbered account. Eventually, the fraction deposits total a significant sum. Data diddling is changing information during input, processing, output, or storage. A virus hoax is a social engineering attack designed to play off of the fears of victims to convince them to perform malicious activities against themselves.

REFERENCES

2.3.1 Social Engineering Overview

2.3.2 Social Engineering Overview Facts

2.3.3 Social Engineering Motivation

2.3.4 Social Engineering Motivation Facts

2.3.5 Social Engineering Techniques

2.3.6 Social Engineering Techniques Facts

2.3.7 Phishing and Internet-Based Techniques

2.3.8 Phishing and Internet-Based Techniques Facts

2.3.9 Use the Social Engineer Toolkit

2.3.10 Investigating a Social Engineering Attack

2.3.11 Identify Social Engineering

5.6.1 Web Threat Protection

5.6.1 Web Threat Protection

5.6.4 Web Threat Protection Facts

13.3.2 Email Security Facts

13.3.3 Protecting a Client from Spam

q_email_sec_spam_01_secp7.question.fex

Question 20: ✓ Correct

Users in your organization receive email messages informing them that suspicious activity has been detected on their bank accounts. They are directed to click a link in the email to verify their online banking username and password. The URL in the link is in the .ru top-level DNS domain.

Which kind of attack has occurred?

○ Buffer overflow

➡ ◉ Phishing

○ Open SMTP relay

○ Virus

EXPLANATION

A phishing scam uses an email that purports to be from a trusted organization and asks you to verify personal information or send money. In a phishing attack:

- A fraudulent message (which appears to be legitimate) is sent to a target.
- The message requests that the target visit a fraudulent website (which also appears to be legitimate). Graphics, links, and web pages look almost identical to legitimate requests from legitimate websites.
- The fraudulent website requests that the victim provide sensitive information, such as an account number and password.

An SMTP relay is an email server that accepts mail and forwards it to other mail servers. In a buffer overflow attack, a program (while writing data to a memory buffer) overruns the buffer's boundaries and writes data in adjacent memory addresses.

REFERENCES

1.2.3 Defense Planning Facts

2.3.1 Social Engineering Overview

2.3.2 Social Engineering Overview Facts

2.3.3 Social Engineering Motivation

2.3.4 Social Engineering Motivation Facts

2.3.5 Social Engineering Techniques

2.3.6 Social Engineering Techniques Facts

2.3.7 Phishing and Internet-Based Techniques

2.3.8 Phishing and Internet-Based Techniques Facts

2.3.9 Use the Social Engineer Toolkit

- 2.3.10 Investigating a Social Engineering Attack
- 2.3.11 Identify Social Engineering
- 5.6.4 Web Threat Protection Facts
- 13.3.2 Email Security Facts

q_email_sec_phishing_01_secp7.question.fex