Chp 14 NS

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/28/2022 9:19:18 am • Time spent: 04:21

Score: 100% Passing Score: 80%

Question 1: ✔ Correct

A recreation of historical events is made possible through which of the following?

- Penetration testing
- Incident reports
- Audits
- ➡ Audit trails

EXPLANATION

The ability to recreate historical events is made possible through audit trails. Without the evidence in an audit trail, knowledge of activities that occurred in the past (minutes or longer) is fairly non-existent.

Audits are the security assessments performed by external auditors to check compliance with security policy and best business practices. Penetration testing is the use of hacker techniques and tools to assess security. An incident report is often produced from audit trails and is an example of the recreation of historical events rather than being the source that makes such reconstruction possible.

REFERENCES

14.1.2 Audit Facts

q_audit_audit_03_secp7.question.fex

Question 2: ✔ Correct

Which ISO publication lays out guidelines for selecting and implementing security controls?

- 27701
- 27001
- 31000
- 27002

EXPLANATION

Publication 27002 lays out guidelines for selecting and implementing security controls.

ISO 27001 is the publication that covers implementing and improving a security management system as well as an assessment guideline.

31000 covers risk management as it pertains to business continuity, safety, environmental results, and the professional reputation of a company.

ISO 27701 covers establishing, implementing, and improving a privacy information management system.

REFERENCES

14.2.4 Security Frameworks Facts

q_sec_frmwk_27002_secp7.question.fex

Question 3: ✔ Correct

When you dispose of a computer or sell used hardware, it is crucial that none of the data on the hard disks can be recovered.

Which of the following actions can you take to ensure that no data is recoverable?

- Encrypt all data on the hard disks.
- ➡ Damage the hard disks so badly that all data remanence is gone.
- Delete all files from all the hard disks in the computer.
- Reformat all the hard disks in the computer.

EXPLANATION

When you dispose of a computer, sell used hardware, or erase important information, it's crucial to destroy all of the data on a device. It's not enough to delete the data. Reformatting the hard drive is also not sufficient. If other people can access the computer, they can use data remanence (the residual representation of erased data) to recover information. You must damage the hardware so badly that the remanence is gone.

REFERENCES

14.3.8 Data Destruction Facts

q_data_destroy_facts_pulv_01_secp7.question.fex

Question 4: ✔ Correct

Which of the following is the LEAST reliable means of cleaning or purging media?

- OS low-level formatting
- Degaussing
- Drive controller hardware-level formatting
- Overwriting every sector with alternating 1s and 0s

EXPLANATION

The least reliable means to clean or purge media is degaussing. Degaussing is the use of strong magnetic fields to remove stored information from a drive. Unfortunately, user error and equipment failure often results in only partially cleaned media.

Various forms of formatting (such as OS low-level formatting and drive controller hardware-level formatting) are not perfect, but they are often more reliable than degaussing. Overwriting every sector with alternating 1s and 0s can be effective if performed multiple times (such as 60 or more).

REFERENCES

14.3.8 Data Destruction Facts

q_data_destroy_facts_degaus_secp7.question.fex

Question 5: ✔ Correct

Your organization has suffered a data breach, and it was made public. As a result, stock prices have fallen, as consumers no longer trust the organization.

Which of the following BEST describes the type of consequence your organization has suffered due to the breach?

- Notifications
- ➡ Reputation damage
- Identity theft
- IP theft

EXPLANATION

This scenario best describes an organization's reputation damage from a data breach. A company's reputation determines if people invest, if consumers buy a product or service, or if foreign governments even allow a certain company to do business in their jurisdiction. A company lives or dies by its revenues and investments, so a breach that exposes client data directly affects the way consumers and investors spend their money. A data breach can cause stock prices to fall, and falling stock prices lead to selloffs and permanent damage.

Notifications are usually sent out following a data breach. This scenario does not describe this.

Intellectual property (IP) is the lifeblood of companies. When their IP is stolen, they lose competitive advantage. This scenario does not describe this.

Identity theft is when a breach occurs and personal information is stolen. The affected individual or entity is forced to do hours of work to correct someone else's mistake.

REFERENCES

14.3.2 Consequences of Breaches Facts

q_breaches_reputation_secp7.question.fex

Question 6: ✔ Correct

Your organization has discovered that an overseas company has reverse-engineered and copied your main product and is now selling a counterfeit version.

Which of the following BEST describes the type of consequence your organization has suffered?

- ➡ IP theft
- Reputation damage
- Escalation
- Fines

EXPLANATION

Intellectual property (IP) is the lifeblood of companies. When their IP is stolen, they lose competitive advantage. The internet has made the world smaller, and companies are now competing with others from around the globe. When IP is stolen through a data breach, it is often sold to competing companies. Many of the companies are overseas and not subject to laws in the United States, making them difficult to prosecute. This allows reverse-engineering or direct copying of IP and gives thieves an undeserved revenue source. This also floods the market with counterfeit goods.

A company's reputation determines if people invest, if consumers buy a product or service, or if foreign governments even allow a certain company to do business in their jurisdiction. This scenario does not describe this.

Fines can be levied against an organization as a result of a data breach. This scenario does not describe this.

Escalation can be separated into two categories, which are internal escalation and external escalation. Internal escalation is part of a company's incident-response plan. External escalation is when experts need to be brought in from the outside to investigate, provide legal counsel, or even enforce laws.

REFERENCES

14.3.2 Consequences of Breaches Facts

q_breaches_iptheft_secp7.question.fex

Question 7: ✔ Correct

If you lose your wallet or purse and it ends up in the wrong hands, several pieces of information could be used to do personal harm to you. These pieces of information include the following:

- Name and address
- Driver license number
- Credit card numbers
- Date of birth

Which of the following classifications does this information fall into?

- Proprietary information
- Private internal information
- ➡ Personally identifiable information (PII)
- Private restricted information

EXPLANATION

Personally identifiable information (PII) is information that can be used on its own or with other information to identify, contact, or locate a single person. This information includes:

- Full name (if not common)
- Home address
- Email address (if private from an association/club membership, etc.)
- National identification number
- Passport number
- IP address (when linked, but it is not PII by itself in US)
- Vehicle registration plate number
- Driver's license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Date of birth
- Birthplace
- Genetic information
- Telephone number
- Login name, screen name, nickname, or handle

Proprietary information is information that a company wishes to keep confidential. Private internal information is restricted to individuals within the organization and can include personnel records, financial records, and customer lists. Private restricted information is restricted to limited authorized personnel within the organization and can include trade secrets, strategic information, and highly sensitive information.

REFERENCES

14.3.4 Information Classification Facts

q_info_class_pii_secp7.question.fex

Question 8: ✔ Correct

Which component of an IT security audit evaluates defense in depth and IT-related fraud?

- ➡ Risk evaluation
- External audit
- User access and rights review
- Financial audit

EXPLANATION

A risk assessment includes an evaluation of:

- Defense in depth.
- Proper governance policies.
- Current redundancy plans.
- Proper use of corporate technology resources.
- Company and IT security strategies, policies, and procedures.
- IT-related fraud.

A user access and rights review, also known as privilege auditing, checks users' and groups' rights and privileges to guard against creeping privileges. Privilege auditing also aids in user and group administration.

An external audit is one performed by an outside auditor that is often done for compliance obligations.

A financial audit is performed to verify compliance with applicable requirements.

REFERENCES

14.1.2 Audit Facts

q_audit_risk_secp7.question.fex

Question 9: ✔ Correct

Which type of control makes use of policies, DPRs, and BCPs?

- ➡ Managerial
- Preventative
- Technical
- Operational

EXPLANATION

Managerial controls consist of management techniques and administrative procedures. These can include security policies, hiring policies, disaster recovery plans (DPRs), and business continuity plans (BCPs).

Operational controls are ones that the security team performs daily.

Technical controls are based around software, applications, and security appliances.

Preventative controls, such as an IPS, are used to prevent security breaches.

REFERENCES

14.2.2 Control Categories and Types Facts

q_ctrl_cattypes_managerial_secp7.question.fex

Question 10: ✔ Correct

Which of the following types of auditing verifies that systems are utilized appropriately and in accordance with written organizational policies?

- ➡ Usage audit
- Internal audit
- PoLP
- Financial audit

EXPLANATION

Usage auditing verifies that systems are utilized appropriately and in accordance with written organizational policies. These audits also ensure that rights are necessary for specific groups. If a granted right isn't used by a group, they may not need access to it.

Internal audits focus on improvement and don't negatively affect customer contracts.

PoLP is the principle of least privilege. It does not apply in this scenario.

Financial audits are performed to ensure compliance with SOX or PCI DSS requirements.

REFERENCES

14.1.2 Audit Facts

q_audit_usage_secp7.question.fex

Question 11: ✔ Correct

Which of the following terms identifies the process of reviewing log files for suspicious activity and threshold compliance?

- CompSec
- Phishing
- Scanning
- ➡ Auditing

EXPLANATION

Auditing is a complement to penetration testing and serves as documentation of attempted attacks that exceed preconfigured thresholds. Most operating systems, network devices, and security packages support the logging of usage data. Examples include the success or failure of login attempts, file access, and administrative tasks. The detailed configuration of audit logs is necessary to ensure that all pertinent data is captured and available for review. Audit logs are sometimes used as evidence in court proceedings.

REFERENCES

14.1.2 Audit Facts

q_audit_audit_01_secp7.question.fex

Question 12: ✔ Correct

Which of the following frameworks introduced the first cloud-centric individual certification?

- CCM
- ISO
- NIST
- CSA

EXPLANATION

The Cloud Security Alliance (CSA) is a relatively new, ten-year-old security framework. With the exponential growth of cloud computing, the need for a cloud security framework was crucial. Along with best practices in cloud security, CSA also introduced the first cloud-centric individual certification.

The Cloud Control Matrix (CCM) is a guide to assist prospective cloud users in evaluating a cloud provider's security risk.

The National Institute of Standards and Technology (NIST) is one of the largest security frameworks. It is used by the federal government and all its departments, including the Department of Defense.

The International Organization for Standardization (ISO) is a worldwide organization that is currently the standardizing body in 164 different countries.

REFERENCES

14.2.4 Security Frameworks Facts

q_sec_frmwk_csa_secp7.question.fex

Question 13: ✔ Correct

Which of the following BEST describes compensating controls?

- Attempts to fix any controls that aren't working properly.
- Monitors network activity and informs the security team of a potential security event.
- Partial control solution that is implemented when a control cannot fully meet a requirement.
- Discourages malicious actors from attempting to breach a network.

EXPLANATION

Compensating controls are a partial control solution that is implemented when a control cannot fully meet a requirement.

Detective controls monitor network activity and inform the security team of a potential security event.

Corrective controls attempt to fix any controls that aren't working properly.

Deterrent controls discourage malicious actors from attempting to breach a network.

REFERENCES

14.2.2 Control Categories and Types Facts

q_ctrl_cattypes_compensating_secp7.question.fex

Question 14: ✔ Correct

To answer this question, complete the lab using the information below.
You have already answered this question.
You are not allowed to view the lab again.

Launch Lab

You completed the lab correctly.

View Lab Report

You are the IT security administrator for a small corporate network. You need to enable logging on the switch in the networking closet.

In this lab, your task is to:

- Enable logging and the Syslog Aggregator.
- Configure RAM Memory Logging as follows:
  - Emergency, Alert, and Critical: **Enable**
  - Error, Warning, Notice, Informational, and Debug: **Disable**
- Configure Flash Memory Logging as follows:
  - Emergency and Alert: **Enable**
  - Critical, Error, Warning, Notice, Informational, and Debug: **Disable**
- Copy the running configuration file to the startup configuration file using the following settings:
  - Source File Name: **Running configuration**
  - Destination File Name: **Startup configuration**

REFERENCES

2.2.6 Configure Microsoft Defender

2.3.11 Identify Social Engineering

3.1.3 Implement Physical Security

4.2.5 Configure Automatic Updates

4.2.7 Configure Microsoft Defender Firewall

4.3.5 Configure NTFS Permissions

4.3.6 Disable Inheritance

5.1.7 Configure a Security Appliance

5.1.8 Configure Network Security Appliance Access

5.1.10 Configure QoS

5.2.3 Configure a DMZ

5.3.5 Configure a Perimeter Firewall

5.4.3 Configure NAT

- 5.5.4 Configure a Remote Access VPN
- 5.5.5 Configure a VPN Connection iPad
- 5.6.3 Configure URL Blocking
- 5.9.6 Secure a Switch
- 5.11.6 Spoof MAC Addresses with SMAC
- 5.11.9 Harden a Switch
- 5.11.10 Secure Access to a Switch
- 5.11.11 Secure Access to a Switch 2
- 5.12.4 Explore VLANs
- 5.13.5 Restrict Telnet and SSH Access
- 5.13.6 Permit Traffic
- 5.13.7 Block Source Hosts
- 6.5.5 Create OUs
- 6.5.6 Delete OUs
- 6.5.10 Create and Link a GPO
- 6.5.11 Create User Accounts
- 6.5.12 Manage User Accounts
- 6.5.13 Create a Group
- 6.5.14 Create Global Groups
- 6.6.4 Configure Account Password Policies
- 6.6.6 Restrict Local Accounts
- 6.6.7 Secure Default Accounts
- 6.6.8 Enforce User Account Control
- 6.6.11 Configure Smart Card Authentication
- 6.7.4 Create a User Account
- 6.7.5 Rename a User Account
- 6.7.6 Delete a User

- 6.7.7 Change Your Password
- 6.7.8 Change a User's Password
- 6.7.9 Lock and Unlock User Accounts
- 6.8.3 Rename and Create Groups
- 6.8.4 Add Users to a Group
- 6.8.5 Remove a User from a Group
- 6.10.6 Configure Kerberos Policy Settings
- 7.1.11 Hide Files with OpenStego
- 7.3.5 Compare an MD5 Hash
- 7.4.3 Encrypt Files with EFS
- 7.4.8 Configure BitLocker with a TPM
- 7.5.6 Manage Certificates
- 8.1.5 Configure a Wireless Network
- 8.2.6 Configure Rogue Host Protection
- 8.3.6 Harden a Wireless Network
- 8.3.7 Configure WIPS
- 8.3.9 Configuring a Captive Portal
- 9.1.6 Create Virtual Machines
- 9.2.6 Create Virtual Switches
- 9.8.4 Secure an iPad
- 9.8.6 Create a Guest Network for BYOD
- 10.1.5 Allow SSL Connections
- 10.3.10 Clear the Browser Cache
- 10.3.15 Perform an SQL Injection Attack
- 10.4.10 Implement Application Whitelisting with AppLocker
- 10.4.12 Implement Data Execution Preventions
- 11.3.5 Implement Intrusion Prevention

- 11.4.7 Scan for Windows Vulnerabilities
- 11.4.8 Scan for Linux Vulnerabilities
- 11.4.9 Scan for Domain Controller Vulnerabilities
- 11.4.10 Scan for IoT Vulnerabilities
- 11.4.11 Scan for WAP Vulnerabilities
- 11.6.4 Poison ARP and Analyze with Wireshark
- 11.6.6 Poison DNS
- 11.6.8 Analyze a SYN Flood Attack
- 11.7.4 Crack Password with Rainbow Tables
- 11.7.7 Crack a Password with John the Ripper
- 12.7.6 Configure Fault-Tolerant Volumes
- 12.8.6 Back Up Files with File History
- 12.8.8 Recover a File from File History
- 12.8.10 Backup a Domain Controller
- 13.3.5 Configure Email Filters
- 13.3.7 Secure Email on iPad
- 14.1.4 Configure Advanced Audit Policy
- 14.1.6 Enable Device Logs

fe9f5de7-0c90-42c7-bfae-adcd1378f576

Question 15: ✔ Correct

Which of the following security frameworks is used by the federal government and all its departments, including the Department of Defense?

- ISO
- CSA
- SOC Type II/III
- NIST

EXPLANATION

The National Institute of Standards and Technology (NIST) is one of the largest security frameworks. It is used by the federal government and all its departments, including the Department of Defense. Security is one of the many verticals that NIST provides guidance for, and NIST's cybersecurity frameworks are the gold standard.

The International Organization for Standardization (ISO) is a worldwide organization that is currently the standardizing body in 164 different countries.

The System and Organization Controls (SOC) is made up of controls and has three types of reports that help a third party determine (through an audit) how a company is adhering to systems and controls.

The Cloud Security Alliance (CSA) is a relatively new, ten-year-old security framework that focuses on cloud security.

REFERENCES

14.2.4 Security Frameworks Facts

q_sec_frmwk_nist_secp7.question.fex

Question 16: ✔ Correct

Which of the following laws was designed to protect a child's information on the internet?

- GDPR
- CCPA
- GLBA
- COPPA

EXPLANATION

The Children's Online Privacy Protection Act of 1998 (COPPA) requires organizations that provide online services designed for kids below the age of 13 (such as websites and gaming sites) to obtain parental consent prior to collecting a child's personal information and using it. This includes such actions as displaying the information on the website, selling it to a marketing company, and so on.

The General Data Protection Regulation (GDPR) is a data-compliance regulation that started in 2018. GDPR provides sweeping changes to the way customer data is treated in the European Union.

The California Consumer Privacy Act (CCPA) was passed in 2020 and was one of the first data privacy acts in the United States.

The Gramm-Leach-Bliley Act (GLBA) is designed to protect private data held at financial institutions.

REFERENCES

14.3.6 Privacy and Responsibility of Data

q_priv_data_resp_coppa_secp7.question.fex

Question 17: ✔ Correct

Which of the following is a collection of recorded data that may include details about logons, object access, and other activities deemed important by your security policy and is often used to detect unwanted and unauthorized user activity?

- ➡ Audit trail
- CPS (Certificate Practice Statement)
- Chain of custody
- Syslog

EXPLANATION

An audit trail is a collection of recorded data that may include details about logons, object access, and other activities deemed important by your security policy that is often used to detect unwanted and unauthorized user activity.

Syslog is a standard protocol for recording system events, not user events. A chain of custody is a document related to evidence-gathering that contains details about personnel in possession and control of evidence from the time of discovery up through the time of presentation in court. A CPS (Certificate Practice Statement) is a document written by a certificate authority that outlines their certificate handling, management, and administration procedures.

REFERENCES

14.1.2 Audit Facts

q_audit_audit_02_secp7.question.fex

Question 18: ✔ Correct

Which of the following describes privilege auditing?

- Users' activities are logged to document incidents for security investigations and incident response.
- ➡ Users' and groups' rights and privileges are checked to guard against creeping privileges.
- An employee is granted the minimum privileges required to perform the duties of his or her position.
- No single user is granted sufficient privileges to compromise the security of an entire environment.

EXPLANATION

Privilege auditing checks users' and groups' rights and privileges to guard against creeping privileges. Privilege auditing also aids in user and group administration.

The principle of least privilege specifies that an employee is granted the minimum privileges required to perform the duties of his or her position. Separation of duties is the security principle that states that no single user is granted sufficient privileges to compromise the security of an entire environment. Usage auditing logs users' activities to document incidents for security investigations and incident response.

REFERENCES

14.1.2 Audit Facts

q_audit_privilege_secp7.question.fex

Question 19: ✔ Correct

Which of the following is true concerning internal audits?

- They are always highly rigorous.
- The process is very formal.
- The auditor works independently.
- ➡ They are generally nonobjective.

EXPLANATION

Internal audits tend to be nonobjective and, consequently, may not be as rigorous.

None of the other answers best describe internal audits.

REFERENCES

14.1.2 Audit Facts

q_audit_internal_secp7.question.fex

Question 20: ✔ Correct

Which of the following government acts protects medical records and personal health information?

- FACTA
- ACA
- HIPAA
- FISMA

EXPLANATION

In the US, you must follow laws dictated by three government acts:

- HIPAA stands for Health Insurance Portability and Accountability Act. HIPAA protects medical records and personal health information. Companies that provide healthcare insurance handle HIPAA-protected information. And, of course, companies that provide health-related services also handle HIPAA-protected information.
- FACTA (Fair and Accurate Credit Transactions Act) was created to protect against identity theft. The act applies to the disposal of consumer reports and related information. FACTA includes credit reports, credit scores, employment history information, check writing history, insurance claims, residential or tenant history, and medical history. Every business handles FACTA-protected information, and every business must comply with FACTA laws.
- FISMA (Federal Information Security Management Act) protects government information. It is primarily concerned with proper data destruction and has detailed disposal requirements.
- ACA is the Affordable Care Act, often referred to as Obamacare.

REFERENCES

14.3.6 Privacy and Responsibility of Data

q_priv_data_resp_hipaa_01_secp7.question.fex

Question 21: ✔ Correct

Which of the following data destruction techniques uses a punch press or hammer system to crush a hard disk?

- Shredding
- Degaussing
- Pulping
- Pulverizing
- Purging

EXPLANATION

The following are various ways to destroy data:

- Burning: the method of building a small fire somewhere legal and safe. Use metal tongs to burn your documents one by one or a few at a time. It's important to ensure that each document is turned into ash. If sensitive information escapes the flames and flies away, it might fall into the wrong hands.
- Shredding: running a hard disk through a disk shredder, physically destroying the drive.
- Pulping: a way of removing all traces of ink from paper by using chemicals and then mashing the paper into pulp. Since these chemicals can ruin carpet and clothing, you should perform this process outside and use protective gloves.
- Pulverizing: like shredding except that it uses a punch press or hammer system to crush a hard disk into a pile of metal confetti.
- Degaussing: purges the hard disk by exposing it to a high magnetic pulse that destroys all of the data on the disk. This also ruins the motors inside the drive.
- Purging: the removal of sensitive data, ensuring that it cannot be reconstructed by any known technique.
- Wiping: a software-based method of overwriting data to completely destroy all electronic data residing on a hard disk drive or other digital media. Wiping uses 0s and 1s to overwrite data onto all sectors of the device. The data is rendered unrecoverable and achieves data sanitization.

REFERENCES

14.3.8 Data Destruction Facts

q_data_destroy_facts_pulv_02_secp7.question.fex

Question 22: ✔ Correct

Which type of control is used to discourage malicious actors from attempting to breach a network?

- Detective
- Physical
- Preventative
- Deterrent

EXPLANATION

The deterrent control type discourages malicious actors from trying to breach a network. The more deterrents are implemented, the less likely it is that anyone tries. These could include internal security policies, access-protected doors for a server room, entry-point access restriction, biometric sensors, man traps, security cameras, security training, and security guards.

Detective controls monitor network activity and inform the security team of a potential security event. Detective controls also log activities and provide artifacts to help investigate the event. Intrusion detection systems are an example of detective controls.

Physical deterrents keep unauthorized people from physically accessing a company's assets. Locked doors, proximity cards, fences, cameras, and guards are all ways to physically protect a network.

Preventative controls, such as an IPS, are used to prevent security breaches.

REFERENCES

14.2.2 Control Categories and Types Facts

q_ctrl_cattypes_deterrent_secp7.question.fex