

Q. Security & Risk Management, a scenario will be the basis for the next few questions and that scenario will be repeated in each question.

Ashley Action is a web content development company with 40 employees located in two offices: one in Ottawa and a smaller office in Toronto. Each office has a local area network protected by a perimeter firewall. The LAN contains modern switch equipment connected to both wired and wireless networks.

Each office has its own file server, and the IT team runs software every hour to synchronize files between the two servers, distributing content between the offices. These servers are primarily used to store images and other files related to web content developed by the company. The team also uses a SaaS based email and document collaboration solution for much of their work.

You are the newly appointed IT manager for Ashley Action and you are working to augment existing security controls to improve the organizations security.

Users in the two offices would like to access each others file servers over the Internet. What control would provide confidentiality for those communications?

Ans: To ensure confidentiality for communications between the two offices of Ashley Action over the Internet, implementing a Virtual Private Network (VPN) would be the most effective control. A VPN establishes a secure and encrypted connection over a less secure network, such as the Internet. This encrypted tunnel ensures that any data transmitted between the two offices is secure from eavesdropping and interception by unauthorized parties.

Here's how it would work in Ashley Action's scenario:

Site-to-Site VPN: Implement a site-to-site VPN to connect the two office networks securely. This creates a virtual bridge between the LANs in Ottawa and Toronto, allowing users to access each other's file servers as if they were on the same local network but with the data being encrypted during transit over the Internet.

VPN Protocols: Use secure VPN protocols like IPSec (Internet Protocol Security) or SSL/TLS (Secure Sockets Layer/Transport Layer Security) for encrypting the data. IPSec is suitable for site-to-site connections, providing strong encryption and authentication.

Firewall Configuration: Configure the perimeter firewalls at both offices to allow VPN traffic. This involves setting up VPN pass-through and possibly opening specific ports (for example, port 500 for IKE in IPSec) while ensuring the firewall continues to block unauthorized access.

Strong Authentication: Implement strong authentication methods for the VPN, such as certificates or two-factor authentication, to ensure that only authorized devices and users can establish a VPN connection.

Regular Monitoring and Updates: Continuously monitor VPN connections for any security threats and keep the VPN software and hardware up to date with the latest security patches.

Q. ESHA Solutions, a medium-sized tech company, specializes in providing cloud-based services for small and medium enterprises. The company has offices in several locations, and its primary assets include servers, customer data, and proprietary software

Company Assets:

Physical Assets: Servers and data centers in various locations

Digital Assets: Customer data, financial records.

Incident: The company discovers that its customer database has been compromised.

Unauthorized access to sensitive customer information, including names, addresses, and payment details, has occurred.

What assets are at risk here and how can their CIA be protected? Justify your responses in the context of CISSP CBK domain #2 (Asset Security)

ANS: In the scenario involving ESHA Solutions, the assets at risk due to the compromise of the customer database include both physical and digital assets:

Physical Assets at Risk:

Servers and Data Centers: The integrity and availability of these assets are at risk. If the compromise involved a breach of the servers where the customer database is hosted, this suggests vulnerabilities that could be exploited to disrupt service or damage the physical infrastructure.

Digital Assets at Risk:

Customer Data: The confidentiality, integrity, and availability of sensitive customer information, including names, addresses, and payment details, are directly at risk. This data breach threatens the privacy and security of the customers.

Financial Records: Although not directly mentioned as compromised, financial records are often targeted following a breach of customer data. The integrity and confidentiality of these records are critical for the company's financial health and trustworthiness.

To protect the Confidentiality, Integrity, and Availability (CIA) of these assets in alignment with CISSP CBK domain #2 (Asset Security), ESHA Solutions should implement the following measures:

Data Encryption: Encrypt sensitive customer data both at rest and in transit. This ensures that even if unauthorized access occurs, the information remains unintelligible and useless to attackers.

Access Control Measures: Implement strict access control measures, ensuring that only authorized personnel have access to sensitive data and systems. This includes the use of multi-factor authentication, least privilege principle, and regular review of access rights.

Regular Security Assessments: Conduct regular vulnerability assessments and penetration testing to identify and remediate security weaknesses in servers, applications, and network infrastructure.

Data Backup and Recovery: Establish robust data backup and recovery procedures to ensure the availability of customer data and financial records in the event of a breach or data loss. Regularly test these procedures to confirm their effectiveness.

Security Awareness Training: Provide ongoing security awareness training for all employees to recognize and respond to phishing attacks and other social engineering tactics that could lead to a breach.

Incident Response Plan: Develop and maintain an incident response plan that includes procedures for responding to data breaches. This plan should be regularly tested and updated to ensure its effectiveness in a real-world scenario.

Regulatory Compliance: Ensure that all measures taken are in compliance with relevant data protection regulations (e.g., GDPR, CCPA) to mitigate legal risks and maintain customer trust.

Monitoring and Detection: Implement continuous monitoring and detection solutions to identify suspicious activities indicative of a breach or attempted breach, enabling rapid response to potential threats.

Q: A medium-sized Managed Service Provider (MSP) called "XYZ" is responsible for managing clients' system admin responsibilities. Accordingly, they have access to the IT infrastructures of multiple companies. XYZ regularly hosts visitors and potential clients at its head office, where they tour the offices where XYZ employees carry out their duties. Unfortunately, some of the employees do not adhere to clear desk policies.

During one such visit, an apparently innocent visitor walked through the office and noticed employee desks (unoccupied at the time) with sticky notes containing information about existing clients, including server IPs, usernames, and passwords. Several months later, a data breach was reported in the networks of these clients, leading to the forced shutdown to halt the intrusion.

Which assets were affected, and how can XYZ better manage their assets?

Remember to link your answer to your learning in the course.

ANS: In the scenario involving XYZ, a Managed Service Provider (MSP), the breach highlights significant lapses in asset management and security practices. The primary assets affected include:

Digital Assets:

Client Information: The confidentiality and integrity of client information, including server IPs, usernames, and passwords, were compromised. This information is critical for maintaining the security of the IT infrastructures of XYZ's clients.

Client IT Infrastructures: The networks and systems of the clients, whose information was exposed, were directly affected. The data breach led to unauthorized access and potential alteration or theft of sensitive data.

Reputational Asset:

XYZ's Reputation: Although not a tangible asset, the trust and reputation of XYZ as a secure and reliable MSP have been severely damaged, impacting its business relationships and future prospects.

To better manage their assets and prevent such incidents in the future, XYZ should implement the following measures, linking back to the principles learned in asset security management:

Enforce a Clear Desk Policy: Strictly enforce a clear desk policy to ensure that sensitive information is not left exposed on desks, especially in areas accessible to visitors. This includes the secure storage of sticky notes, documents, and any other media containing sensitive information when not in use.

Access Control and Visitor Management: Implement stricter access control measures to restrict visitor access to sensitive areas within the office. This could include escorted tours, designated visitor areas, and badge access systems to ensure that visitors cannot wander unattended.

Employee Awareness and Training: Regularly conduct security awareness training for all employees, emphasizing the importance of adhering to security policies, including the clear desk policy and the handling of sensitive information. This training should also cover recognizing and mitigating social engineering attacks.

Physical Security Measures: Enhance physical security measures to monitor and control access to the office premises. This may include surveillance cameras, secure locking mechanisms, and alarm systems to deter unauthorized access.

Secure Information Management Practices: Implement secure information management practices, such as encryption for digital files, secure password management tools instead of writing passwords on sticky notes, and the use of secure channels for sharing sensitive information.

Regular Security Audits: Conduct regular security audits to assess compliance with security policies and identify vulnerabilities in physical and information security practices. This should include a review of how sensitive information is handled and stored.

Incident Response Plan: Develop and regularly update an incident response plan that includes procedures for responding to data breaches and information leaks. This plan should outline steps for containment, investigation, notification, and recovery, as well as lessons learned to improve future security.

Client Communication and Transparency: Maintain open lines of communication with clients regarding security policies and practices. In the event of a breach, being transparent and proactive in addressing the issue can help mitigate damage to trust and reputation.

By addressing these areas, XYZ can significantly enhance its asset management and security practices, protecting both its own and its clients' assets from future threats. These measures align with the principles of asset security management, emphasizing the importance of both physical and information security in safeguarding sensitive information.

Q: Which of the following security models is responsible for evaluating network protocols and encryption methods used to ensure confidentiality and integrity of network communications?

Ans : Orange Book

Q: Which of the following is a legal device that gives the creator of a work the right to control how the work is used?

ChatGPT

The legal device that gives the creator of a work the right to control how the work is used is **copyright**.

Q: Cyberlaw categorizes computer-related crime into three categories. Which of the following is an example of a crime in which the use of a computer would be categorized as incidental?

ANS: Capturing passwords as they are sent to the authentication server

Q: Which of the following policies is required when industry standards or government legislations apply to your company?

Ans: Regulatory

Q: What feature enables code to be executed without the usual security checks?

Ans: Maintenance hook

The ratings of the top five intrusion detection system products are being researched for deployment by a company. Which of the following are the evaluation criteria most in use today for these types of purposes?

Ans: Common Criteria

Q: Which model deals only with confidentiality?

Ans: Bell-LaPadula

Q: The operating system performs all except which of the following tasks?

Ans: User access to database views

In the *(star) property of the Bell-LaPaluda model,

Subjects cannot read from a higher level of security relative to their level of security

Subjects cannot read from a lower level of security relative to their level of security

Subjects cannot write to a higher level of security relative to their level of security

Subjects cannot read from their same level of security

Ans: Subjects cannot write to a higher level of security relative to their level of security. (True)

The *security property of which of the following models ensures that a subject with clearance level of "secret" has the ability to write only to a set of objects and in order to prevent disclosure, the subject may write to objects classified as "secret" or "top secret" but is prevented from writing information classified as "public".

Ans: Bell-LaPudula

Q: What is the best definition of a security model?

Ans: A security model provides a framework to implement a security policy

Q: The trusted computing base (TCB) controls which of the following?

Ans: All trusted processes and software components

Q: Which security architecture model defines how to securely develop access rights between subjects and objects?

Ans: Clark-Wilson

Q: This portion of the CPU performs arithmetic and logical operations on the binary data.

Ans: ALU

Q: In systems utilizing a ring protection scheme, at what level does the security kernel reside?

Listen

Ans: Level 0

Q: On a computer system primary storage is the:

Ans: Memory directly addressable by the CPU, which is for the storage of instructions and data that are associated with the program being executed.

Q:What does the Bell-LaPadula model not allow?

Ans: Subjects to read from a higher level of security relative to their level of security

Q: I/O drivers and utilities are typically found at what protected ring level?

Listen

Ans: Ring 0

Q What is system accreditation?

Ans: Formal acceptance of a stated system configuration

Q. Which of the following are developed by programmers and used to allow the bypassing of normal processes during development?

Ans: Buffer overflows

Q: What security model is also known as the Chinese Wall?

Ans: Brewer and Nash

Q: What is the type of multitasking used in most modern operating systems?

Ans: Preemptive

Q: Processes are placed in a ring structure according to:

Ans: Least privilege

Q: Biba model rule "An object at one level of integrity is not permitted to modify (write to) an object of a higher level of integrity (no write up)" is called

Ans: The simple Integrity Axiom

Q: ISO27001 evolved from what regional standard?

Ans: British Standard 7799

Q: Processes are placed in a ring structure according to:

Ans: Least privilege

Q: To which of the following is the principle of least privilege NOT applicable

Ans: None of the above

Q: What security advantage does firmware have over software?

Ans: It is difficult to modify without physical access

Q: Which of the following describes the rules that need to be implemented to ensure that security requirements are met?

Ans: Security policy

Q: Without proper definition of security requirements, systems fail. Which of the following can be used to capture detailed security requirements?

Ans: All of the above

Q: Access to a Cloud environment always costs more money compared to a traditional desktop environment.

Ans: False

Q: "A program in execution" is the classic definition of a

Ans: process

Q: What is the final step in authorizing a system for use in an environment?

Certification

Ans: Accreditation

Q:Cloud:

is the feature of cloud computing that allows the service to change in size or volume in order to meet a user's needs.

Ans: Scalability

Q: What is a trusted computing base (TCB)?

Ans:The combination of hardware, software, and controls that work together to

Q: The Clark-Wilson model focuses on data's:

Ans: Integrity

Q: The two basic classes of I/O devices are

Ans: block and character

Q: Security & Risk Management: A startup company situated in the notorious tornado alley of the United States is valued at \$600,000. Based on historical data a devastating tornado is likely to affect the area where the company is situated once every ten years. It is projected that such a tornado would destroy 70% of the facility, company assets and endanger life given its construction; the current detective: prevention and means of escape controls in place.

What is the annualized loss expectancy (ALE)?

Ans: 42,000

420,000

To calculate the Annualized Loss Expectancy (ALE), we use the formula:

$$\text{ALE} = \text{Single Loss Expectancy (SLE)} \times \text{Annualized Rate of Occurrence (ARO)}$$

Given:

$$\text{Single Loss Expectancy (SLE)} = \text{Value of the company} \times \text{Percentage of loss (70\% in this case)} = \$600,000 \times 0.70 = \$420,000$$

$$\text{Annualized Rate of Occurrence (ARO)} = 1 \text{ tornado every 10 years} = 1/10 = 0.1$$

Now,
$$\text{ALE} = \$420,000 \times 0.1 = \$42,000$$

So, the Annualized Loss Expectancy (ALE) is \$42,000.

Q: Ashley Action is a web content development company with 40 employees located in two offices: one in Ottawa and a smaller office in Toronto. Each office has a local area network protected by a perimeter firewall. The LAN contains modern switch

equipment connected to both wired and wireless networks.

Each office has its own file server, and the IT team runs software every hour to synchronize files between the two servers, distributing content between the offices.

These servers are primarily used to store images and other files related to web content developed by the company. The team also uses a SaaS based email and document collaboration solution for much of their work.

You are the newly appointed IT manager for Ashley Action and you are working to augment existing security controls to improve the organizations security.

Users in the two offices would like to access each others file servers over the Internet. What control would provide confidentiality for those communications?

Digital signatures

Ans: Virtual private network

Q: Harvey is the risk manager for Collingwood Landing, resort community in Ontario

The resorts main data centre is located in part of the USA known for tornados. Harvey recently undertook a replacement cost analysis and determined that rebuilding and reconfiguring the data centre would cost \$10 million USD.

Harvey consulted with tornado experts, data centre specialist and structural engineers. Together they determined that a typical tornado would cause approximately \$5 million USD of damages to the facility. The meteorologist determined that the Collingwood facility lies in an area where they are likely to experience a tornado once every 200 years.

Based upon the information in this scenario, what is the exposure factor for the effect of a tornado on the Collingwood Landing data centre?

Ans: 50%

The Exposure Factor (EF) represents the percentage of loss that would occur if a particular risk event were to happen. In this scenario, the EF for the effect of a tornado on the Collingwood Landing data centre is calculated as follows:

$EF = (\text{Potential loss due to a tornado}) / (\text{Total value of the data centre})$

Given:

Potential loss due to a tornado = \$5 million USD

Total value of the data centre = \$10 million USD

$EF = (\$5 \text{ million USD}) / (\$10 \text{ million USD}) = 0.5 = 50\%$

So, the Exposure Factor for the effect of a tornado on the Collingwood Landing data centre is 50%.

Q: Harvey is the risk manager for Collingwood Landing, resort community in Ontario.

The resorts main data centre is located in part of the USA know for tornados. Harvey recently undertook a replacement cost analysis and determined that rebuilding and reconfiguring the data centre would cost \$10 million USD

'age 1:

1

Harvey consulted with tornado experts, data centre specialist and structural engineers. Together they determined that a typical tornado would cause approximately \$5 million USD of damages to the facility. The meteorologist determined that the Collingwood facility lies in an area where they are likely to experience a tornado once every 200 years.

Page 2:

2

Page 3:

Based upon the information in this scenario, what is the annualized rate of occurrence for a tornado at Collingwood Landing's data centre?

Ans: 0.005

ChatGPT

To calculate the Annualized Rate of Occurrence (ARO), we use the formula:

$$\text{ARO} = 1 / (\text{Frequency of occurrence})$$

Given that the Collingwood Landing data centre is likely to experience a tornado once every 200 years:

$$\text{ARO} = 1 / 200 = 0.005$$

So, the Annualized Rate of Occurrence (ARO) for a tornado at Collingwood Landing's data centre is 0.005.

Q: These servers are primarily used to store images and other files related to web content developed by the company. The team also uses a SaaS based email and document collaboration solution for much of their work.

You are the newly appointed IT manager for Ashley Action and you are working to augment existing security controls to improve the organizations security.

Finally, there are historical records stored on the server that are extremely important to the business and should never be modified. You would like to add an integrity control that allows you to verify on a periodic basis that files were not modified.

What control can you add?

Ans: Hashing

Q The Biba model rule that states "An object at one level of integrity is not permitted to modify (write to) an object of a higher level of integrity (no write up)" is called "**The *-star) Integrity Axiom.**"

Q: The statement that correctly identifies a problem with sanitization methods is:

"Personnel can perform sanitization steps improperly."

Q: The distribution model in which applications are hosted by a service provider and made available to users is known as Software-as-a-Service (SaaS).

Q: A multi-level storage scheme in which faster media hold the data that are accessed more often, and the seldom-used data are stored on slower devices is referred to as Hierarchical Storage Management (HSM).

Q: Before reusing classified media in a less secure environment, an administrator would "purge" the media. This process is intended to remove stored data in such a way that it cannot be recovered by any means.

Q: The true statement about cloud computing is:

"You can access your data from any computer as long as you have an internet connection."

Q: The most reliable method of destroying data on a solid state drive (SSD) is **purging**. This often involves using specialized software to overwrite the SSD multiple times to ensure the data cannot be recovered. Degaussing is not effective on SSDs as it is on magnetic storage like hard drives, because SSDs do not store data magnetically.

Q: The role of the Chief Information Security Officer (CISO) includes establishing the overall goals of the company security program, ensuring that the company's information assets and technologies are adequately protected. The CISO is typically responsible for the overall vision and strategy of the organization's cybersecurity program.

Q: Data classification is typically the responsibility of the data owner. The data owner is usually a member of management who is in charge of the data and responsible for ensuring it is classified according to the organization's policies and guidelines.

Q: The primary purpose of information classification processes is to define the requirements for protecting sensitive data. This involves categorizing data based on its level of sensitivity and applying appropriate controls to ensure its confidentiality, integrity, and availability.

Q: The statement provided in the image is false. Access to a cloud environment does not always cost more money compared to a traditional desktop environment. Cloud services can often be more cost-effective due to their scalability, reduced need for physical infrastructure, and pay-as-you-go pricing models.

Q:

ISO/IEC 27001 evolved from the British Standard 7799 (BS 7799).

Q: If a component fails, a system should be designed to "**Change to a more secure state.**" This principle is part of designing systems to be resilient and to prevent a failure from escalating into a security breach.

Q: The Biba security model addresses "**Unauthorized modification of data.**" It is designed to prevent data from being written to by a lower integrity level to maintain the integrity of the data.

Q: The Biba model rule "An object at one level of integrity is not permitted to modify (write to) an object of a higher level of integrity (no write up)" is called "The * (star) Integrity Axiom."

Q: The security architecture model that defines how to securely develop access rights between subjects and objects is the Clark-Wilson model. This model is focused on ensuring that subjects (users) can only perform actions on objects (data) in ways that maintain data integrity, enforcing well-formed transactions and separation of duties.

Q: In secure computing systems, there is a logical form of separation used between processes so that each process is contained within its own security domain, preventing unauthorized access to other processes or their resources. This separation ensures that processes operate within their assigned privileges and cannot interfere with each other, enhancing the overall security of the system.

Q: The organizational role that is typically tasked with determining which sensitivity scheme to use is "Management." Management is responsible for defining the classification levels of data and determining the controls that should be applied based on the sensitivity of the data.

Q: Among the options given, "**Remanence**" does not erase data. Remanence refers to the residual representation of digital data that remains even after attempts to erase or clear the data. The other terms listed are methods used to remove or overwrite data