Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING
END TERM EXAMINATION - JUN 2023

Semester : Semester IV - 2021
Course Code : CSE2060
Course Name : Sem IV - CSE2060 - Information Security and Management
Program : CBD,ISD&IST

Date : 21-JUN-2023
Time : 9.30AM - 12.30PM
Max Marks : 100
Weightage : 50%

Instructions:
(i) Read all questions carefully and answer accordingly.
(ii) Question paper consists of 3 parts.
(iii) Scientific and non-programmable calculator are permitted.
(iv) Do not write any information on the question paper other than Roll Number.

PART A

ANSWER ALL THE QUESTIONS **(10 X 2 = 20M)**

1. A highly secure research laboratory is handling classified information related to national security. The management wants to implement a strict access control mechanism with predefined security policies and rules to ensure that only authorized individuals can access the sensitive data. Which access control mechanism would you recommend and how it will enhance security in the research laboratory's.

(CO4) [Knowledge]

2. A company is conducting a risk assessment for a new project they are undertaking. The goal is to identify and evaluate potential risks associated with the project and develop a risk management plan. As part of the risk assessment process, the company uses a risk assessment matrix to assess the likelihood and impact of identified risks. How a risk assessment matrix is used in the risk assessment process?

(CO3) [Knowledge]

3. The network administrator of a corporation observes odd network traffic patterns. Further analysis reveals that numerous networked devices are receiving suspect data packets from an IP address that is associated with a reliable external partner. The administrator suspects an attack might be taking place. In the above circumstance, what kind of attack is the administrator suspecting and how may it be recognized?

(CO2) [Knowledge]

4. To improve its information security procedures, a sizable financial organization is putting a data classification model into effect. What is the information security data classification model employed by this financial institution.

(CO3) [Knowledge]

5. A company's website becomes a target of an attack, rendering the website inaccessible to users. Identify the type of attack in this scenario and discuss the potential consequences for the company.

(CO2) [Knowledge]

6. In an online marketplace, a customer purchases a product from a seller and makes the payment through a secure payment gateway. The transaction is successfully completed, and both parties receive confirmation of the transaction. However, the seller later claims that they never received the payment and demands the customer to make the payment again. The customer insists that they made the payment as evidenced by the transaction confirmation. What kind of security principle is discussed in the scenario and what benefit does this scenario demonstrate?

(CO1) [Knowledge]

7. A technology company has a zero tolerance policy for data breaches and information security incidents. They prioritize the protection of sensitive data and aim to maintain a secure environment for their systems and networks.Explain the concept of zero tolerance risk exposure in the context of information security.

(CO3) [Knowledge]

8. An access control mechanism has been established by a software development company to regulate access to their source code repository. Access permissions for the projects that they are working on can be managed by each developer. Which access control system would the business use to enable developers to restrict access permissions in the source code repository of the software development company.

(CO4) [Knowledge]

9. In a cybersecurity event, an external attacker infiltrates a company's network and launches various destructive actions, such as distributed denial of service (DDoS) attacks and malware distribution via remote devices. What are these remote devices and how do they work?

(CO1) [Knowledge]

10. An attacker group launches a distributed denial of service (DDoS) attack against a government website in response to a new law. Who are the assailants in this group? What is the purpose of this attack, and what consequences will it have on the intended website?

(CO2) [Knowledge]

PART B

ANSWER ALL THE QUESTIONS **(5 X 10 = 50M)**

11. You are a risk manager working for a manufacturing company. The company is planning to expand its operations to a new geographical location. As part of your role, you are responsible for managing the risks associated with the expansion project. Describe the risk management process you would follow to effectively manage the risks associated with the company's expansion to a new geographical location.

(CO3) [Comprehension]

12. Orbit Corporation is a rapidly growing technology startup that operates in a highly competitive industry. They have recently developed an Information Security (IS) policy to protect their intellectual property, customer data, and maintain the trust of their clients. What characteristics of the IS policy has Orbit Corporation developed and how will each characteristics help the corporation in ensuring effective information security management?

(CO1) [Comprehension]

13. MHD Corporation is a large financial institution that deals with sensitive customer data and conducts various financial transactions. They have recently experienced a significant security breach, resulting in the loss of valuable customer information and financial data. Further investigation revealed that the breach was caused by a employee inside the organization. The incident has raised concerns within the organization about the different types of threats that can pose risks to their operations and data. Analyze the scenario and provide a detailed explanation of the different types of threats that organizations should be aware of and the multi-layered strategies to mitigate such threats.

(CO2) [Comprehension]

14. A multinational technology company is planning to expand its operations into a new country with a highly competitive market. However, there are several risks associated with this expansion, including economic instability, political uncertainties, cultural differences, and intellectual property theft. As a risk management consultant, describe the risk management strategies the company can employ to effectively mitigate, accept, transfer, and avoid these risks Explain the risk management strategies that the technology company can implement to effectively mitigate, accept, transfer, and avoid the risks associated with expanding into a new country.

(CO4) [Comprehension]

15.

- John, an employee at XYZ Corporation, receives a suspicious email containing a link. Curious, he clicks on the link, unknowingly activating a malware that encrypts the company's critical files. The malware threatens to delete the files unless a ransom is paid. Identify the Asset, Threat, Threat Vector, Vulnerability, Attack Vector, Likelihood, Risk in the above scenario and justify your answer.
- A hacker gains access to an organization's network and launches a distributed denial-of-service (DDoS) attack, causing the organization's website and online services to become unavailable. Identify the asset, threat, and vulnerability in this scenario. Which security principle would have mitigated this threat? Explain how

(CO2) [Comprehension]

PART C

ANSWER ALL THE QUESTIONS **(2 X 15 = 30M)**

16. A multinational corporation, GlobalTech, has recently experienced a series of security incidents. As a security analyst, you are tasked with analyzing and classifying each incident as either an active attack or a passive attack. Analyze each incident and classify them as either an active attack or a passive attack. Justify your classification by explaining the characteristics of each attack type and how they align with the incidents described.

Incident 1: An unauthorized user gains physical access to GlobalTech's server room and steals a backup tape containing sensitive customer data.

Incident 2: A hacker conducts a brute force attack on GlobalTech's email server, attempting to gain access to employee email accounts by systematically trying various combinations of usernames and passwords.

Incident 3: An employee accidentally sends an email containing sensitive company information to the wrong recipient. The recipient, who is not authorized to access the information, promptly notifies GlobalTech's IT department.

Incident 4: A malicious insider within GlobalTech's organization intentionally alters financial records stored in the company's database to cover up fraudulent activities.

Incident 5: GlobalTech's network traffic is monitored by an external attacker, who captures and analyzes the data to gather information about the company's operations, without directly disrupting the network.

(CO2,CO1) [Application]

17. You are a Security Analyst at TechGuard Corporation, and your CIO has requested you to conduct a risk analysis for a potential security investment. The company operates a cloud-based platform that hosts customer data, including personal and financial information. The platform is composed of 6 servers, each valued at $50,000, and the total value of the customer data is estimated at $2 million. Over the past year, there have been 8 security incidents, with an average cost of $25,000 per incident. The company is considering two countermeasures: Countermeasure A involves implementing data encryption on the servers, which would cost $20,000 per year, and Countermeasure B involves conducting regular security assessments and penetration testing, which would cost $30,000 per year. Calculate the necessary values for each countermeasure and suggest which is the best measure and justify

Quantitative Risk Assessment			Countermeasure	
		Base Case	A	B
Asset Value	AV			
Exposure Factor	EF			
Single Loss Expectancy	SLE			
Annualized Rate of Occurrence	ARO			
Annualized Loss	ALE			
ALE Reduction for Countermeasure	--			
Annualized Countermeasure Cost	--			
Annualized Net Countermeasure Value	--			

(CO3) [Application]