Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING
END TERM EXAMINATION - JUN 2023

Semester : Semester VI - 2020
Course Code : CSE2060
Course Name : Sem VI - CSE2060 - Information Security and Management
Program : CSG

Date : 14-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. John works in a busy coworking environment where employees from several businesses share a common office. He frequently observes a person standing behind him, appearing to pay close attention to his computer screen as he works on private documents. What potential danger is John exposed to in the present scenario? Identify it and explain it.

(CO2) [Knowledge]

2. A multinational organization operates in various sectors, including finance, healthcare, and technology. The company recognizes the importance of effective risk management in safeguarding its assets, ensuring business continuity, and complying with industry regulations. As part of their commitment to risk management, they decide to develop a detailed documentation outlines an organization's approach. In the given scenario, what should they develop and what purpose does it serve for the organization?

(CO3) [Knowledge]

3. A technology company is planning to migrate its entire IT infrastructure to a cloud-based solution. The company wants to assess the potential risks associated with this migration and decide on the necessary risk mitigation measures. They are considering use a subjective and non-mathematical model-based assessment as part of their risk management process. In the context of the technology company's migration to a cloud-based solution, which model do you suggest, and how can it help them evaluate and address the risks involved?

(CO3) [Knowledge]

4. There is a need for a highly secure access control architecture in a government organization that can manage complicated and dynamic information sharing requirements across several hierarchical security levels. The company is thinking about installing an access control system to suit their requirements. Recommend an access control system and describe how it satisfies the needs of the government agency for information sharing.

(CO4) [Knowledge]

5. Sophia is an employee at a large technology company. One day, she receives an email with an attachment claiming to be an important document from her manager. The email is unexpected, but it seems legitimate as it includes the company logo and appears to be written in her manager's style. Without giving it a second thought, Sophia opens the attachment, thinking it is work-related. Unbeknownst to her, the attachment contains malicious code that installs a hidden program on her computer. What type of security threat is Sophia facing in this scenario, and what risks are associated with the presence of this hidden program on her computer?

(CO2) [Knowledge]

6. A company grants excessive access privileges to its employees, allowing them to access and modify data beyond their job requirements. As a result, a user unintentionally deletes critical files, causing a significant disruption to business operations. Which fundamental security principle has been violated in this scenario and how can this violation be defended or mitigated?

(CO1) [Knowledge]

7. In a software development company, the development team is working on a new web application that will handle sensitive customer data. As the security analyst, you are responsible for ensuring software assurance throughout the development process. Identify at least three software assurance practices that can be implemented during the software development lifecycle.

(CO1) [Knowledge]

8. A disgruntled employee deliberately sabotages the company's computer network, causing significant disruptions to operations and data loss. Explain the concept of sabotage or vandalism in this scenario and discuss the potential impact on the organization.

(CO4) [Knowledge]

9. Abacus Corporation has a network infrastructure that includes multiple departments, servers, and workstations. They want to implement a security measure to control and monitor incoming and outgoing network traffic, as well as protect their internal resources from unauthorized access and potential threats. How can Abacus Corporation achieve this information security goal?

(CO3) [Knowledge]

10. A malicious insider threatens to release sensitive company information unless a large sum of money is paid. Identify the type of attack in this scenario and discuss the potential consequences for the targeted organization.

(CO2) [Knowledge]

PART B

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

11. SARCO Company is a software development firm that creates and deploys various software applications for its clients. They prioritize the security of their software products and aim to protect them against potential software attacks. In this scenario, please answer the following questions:Define what software attacks are and explain their significance in the context of information security. b. Identify and describe three common types of software attacks that SaRCO Company should be aware of and defend against in their software applications.Please provide your response based on your knowledge of software attacks and their significance in information security.

(CO2) [Comprehension]

12. A small technology startup is in the process of developing a new web application that will handle sensitive user data. The company wants to conduct a thorough risk assessment to identify potential threats and vulnerabilities associated with the application and prioritize mitigation efforts. The security team decides to use a Threat and Vulnerability Assessment (TVA) worksheet to facilitate the process Describe the components of a TVA worksheet and discuss how they can be utilized in the risk assessment process. Provide a step-by-step solution for conducting a risk assessment using a TVA worksheet in the given scenario.

(CO3) [Comprehension]

13. You are a software developer working for a software development company that follows the NIST (National Institute of Standards and Technology) approach to securing the Software Development Life Cycle (SDLC). In the given scenario, demonstrate how the NIST approach can be applied by answering the following questions: Identify and explain the key stages of the SDLC according to the NIST approach. Discuss the security considerations and activities that should be addressed in each stage. Provide an example of how a specific security control or best practice can be implemented at one stage of the SDLC according to the NIST approach.

(CO1) [Comprehension]

14. A manufacturing company is considering implementing a new automated production system that involves integrating robotics and artificial intelligence. The company's management is concerned about the potential risks associated with this technology. They want to understand the concepts of residual risk, risk appetite, and risk tolerance to make an informed decision. Explain the concepts of residual risk, risk appetite, and risk tolerance using the scenario of the manufacturing company considering the implementation of an automated production system.

(CO4) [Comprehension]

15. A company's finance department receives an email from an unknown sender claiming to be a client and requesting confidential financial information. The email looks legitimate, with the sender using the client's name and mentioning specific details about their business relationship. The employee, unaware of the risks, replies to the email and provides the requested information. Identify and discuss two different types of passive attacks demonstrated in the scenario. Provide detailed explanations of each type, how they are executed, and the potential risks they pose to the company's security.

(CO2) [Comprehension]

PART C

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

16. You are a Security Analyst at TechSolutions Inc., and your CIO has requested you to conduct a risk analysis for a countermeasure to protect the company's intellectual property (IP) from unauthorized access. The company has two research and development facilities, each with 50 workstations. Each workstation is valued at $10,000, and the IP is estimated to be worth $2,000,000. In the past year, there were 8 security incidents, each costing $50,000 on average. A single security incident could potentially result in the loss of 75% of the IP. The company is considering two countermeasures: Countermeasure A involves implementing data encryption for all IP files, which would cost $50,000 per year. Countermeasure B involves conducting regular security awareness training for employees, 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]

17. A financial institution, SecureBank, has experienced several security incidents. Your task as a security analyst is to analyze and classify 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: A group of hackers gain unauthorized access to SecureBank's online banking platform and initiate fraudulent transactions, transferring funds from customer accounts to offshore locations.

Incident 2: An employee receives a malicious email attachment and unknowingly installs ransomware on their workstation. The ransomware encrypts critical files and demands a ransom payment for their release.

Incident 3: A physical breach occurs at one of SecureBank's branch offices, where an attacker gains access to the server room and steals backup tapes containing sensitive customer data.

Incident 4: A hacker intercepts network traffic between SecureBank's ATM machines and the central banking system, collecting customers' card information for later unauthorized use.

Incident 5: An insider intentionally leaks confidential customer financial information to a competitor, compromising the integrity and confidentiality of customer data.

(CO2,CO1) [Application]