NPTEL ASSIGNMENT

Cyber security and privacy

WEEK-1

1. A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source is:
   a. Spear Phishing
   b. Man in the Middle Attack
   c. Smurf Attack
   d. Social media phishing

2. A malicious attack where hackers encrypt an organization's data and demand payment to restore access is known as:
   a. Spyware
   b. Ransomware
   c. Whaling
   d. Watering hole attack

3. Which of the following characteristics are most likely to be found in a phishing email?
   a. Sense of urgency and immediate action requests.
   b. Unusual or inappropriate requests
   c. Incorrect sender name or email address
   d. All of the above.

4. From a managerial perspective, Information Security is generally understood as a:
   a. Product
   b. Technology
   c. Process
   d. Product, Technology and Process

5. The practice of keeping an organization's network infrastructure secure from unauthorized access is known as:
   a. Data Security
   b. Network Security
   c. Information Security
   d. Operations Security

6. Which of the following statements most accurately reflects the complex role of technology in cybersecurity?
   a. Technology acts as both a source of threats and a tool for defense.
   b. Technology is solely a source of threats and vulnerabilities.
   c. Technology plays a triple role: source of threats, asset to protect, and defense weapon.
   d. Technology solely serves as a defense weapon against cyberattacks.

7. _____ is a manipulation technique that exploits human weakness to gain private information, access, or valuables
   a. Spyware
   b. Logic Bomb
   c. Social Engineering
   d. Man in the Middle Attack

By- Saurav kumar

8. True or False: The word "Cyber" in "Cybernetics" originates from the French language.
   a. True
   b. False
9. The impact of a cyber security incident on organizations can include:
   a. Financial Loss
   b. Reputation Damage
   c. Regulatory fine
   d. All the above

10. True or False: A Vendor guarantees that their IoT solutions are 100% safe from cyberattacks. This statement can be
   a. True
   b. False

NPTEL ASSIGNMENT

WEEK-2

1. CIA triad refers to:
   a. Confidentiality, Integrity and Availability
   b. Confidentiality, Integrity and Authentication
   c. Confidentiality, Integrity and Authorization
   d. Cybersecurity, Investigation and Authentication

2. What aspect emerges from the intersection of 3 components of Information Security?
   a. Technology
   b. Policy
   c. Human Security
   d. None of the above

3. ----------, authentication and authorization are means to ensure CIA.
   a. Investigation
   b. Identification
   c. Classification
   d. Verification

4. Should all 27 cells of Mc Cumber's Cube be addressed with the same priority?
   a. True
   b. false

5. Which of the following is/ are the design principles of high availability systems?
   a. Eliminate single points of failure
   b. Ensure reliable crossover
   c. Identify failures in real time
   d. All the above

6. In ensuring confidentiality, what is the crucial process that involves classifying information and individuals, and mapping them based on the level of access
   a. Identification
   b. Authentication

c. Authorization
d. Encryption

7. In addition to cryptography, a number of measures may be used for confidentiality, including:
   a. Information classification
   b. Secure document storage
   c. Application of general security policies
   d. All the above

8. When a control provides assurance that every activity undertaken can be attributed to a named person or automated process, it is known as:
   a. Integrity
   b. Accountability
   c. Accessibility
   d. Authenticity

9. Identify the components of Information Security
   a. Network Security
   b. Computer & Data Security
   c. Management of Information Security
   d. All of the above

10. Which are the three types of power Mc Cumber's Cube identifies?
    a. Technologies
    b. Policies and Practices
    c. People
    d. All the above

NPTEL ASSIGNMENT

WEEK-3

1. The process of defining and specifying the long-term direction to be taken by an organization, and the allocation and acquisition of resources needed to pursue this effort is known as:
   a. Governance
   b. Security Management
   c. Strategic Planning
   d. Objectives

2. Which of the following statements best describes the relationship between GRC (Governance, Risk, and Compliance) and cybersecurity ?
   a. GRC focuses solely on cybersecurity management and overlooks other risk management initiatives.
   b. Cybersecurity is the primary focus of GRC, with minimal consideration for other risks.
   c. GRC integrates cybersecurity as one component within the broader framework of enterprise risk management (ERM).
   d. GRC is a standalone framework independent of cybersecurity and risk management.

3. A written document provided by management that inform employees and others in the workplace about proper behaviour regarding the use of information and information assets are known as:
   a. Guidelines
   b. Information Security Policy
   c. De facto standard
   d. Practices

4. Which approach to cybersecurity management treats cybersecurity as a separate category distinct from other risks an organization may face, and focuses solely on cybersecurity, depending on the size and nature of the organization?
   a. Standard Driven Approach
   b. Organization Planning Approach
   c. GRC Framework
   d. Risk Management Framework

5. Benefits of implementing a GRC in an organization include:
   a. Responsible operations
   b. Data-driven decision-making
   c. Improved cybersecurity
   d. All the above

6. What is the purpose of the COBIT maturity model?
   a. To assess an organization's maturity in IT governance processes
   b. To rank organizations based on their financial performance
   c. To determine the efficiency of network infrastructure
   d. To evaluate employee satisfaction levels in the IT department

7. COSO's ERM framework emphasizes:
   a. Operational efficiency
   b. Risk identification and assessment
   c. Regulatory compliance
   d. Human resource management

8. Which characteristic distinguishes the approaches of COBIT, COSO, and COSO-ERM from specific standards like ISO or NIST?
   a. They prioritize cybersecurity over other risk management aspects.
   b. They focus exclusively on small to medium-sized enterprises (SMEs).
   c. They operate at the enterprise level rather than focusing on specific standards.
   d. They are primarily developed by governmental regulatory bodies.

9. Why might some countries be hesitant to adopt the ISO 27001 model?
   a. It is a mandatory standard with strict compliance requirements.
   b. It is not recognized as a valid security framework by international organizations.
   c. There are concerns about the model's overall effectiveness compared to existing approaches.
   d. It prioritizes specific security vendors or technologies.

10. Which of the following is not considered a principle or practice for securing IT systems?
    a. Implement layered security to ensure there is no single point of vulnerability.
    b. Do not implement unnecessary security mechanisms.
    c. Maximize the system elements to be trusted.
    d. Assume that external systems are insecure.

NPTEL ASSIGNMENT

WEEK – 4

1. A facility that provides only rudimentary services, with no computer hardware or peripherals is known as:
   a. Cold site

b. Hot site
c. Service bureau

2. The amount of effort necessary to make the business function operational after the technology element is recovered is known as:
   a. Recovery Time Objective
   b. Work Recovery Time
   c. Maximum Tolerable Downtime
   d. Recovery Point Objective

3. Contingency Planning includes:
   a. Incident response plan
   b. Disaster recovery plan
   c. Business continuity plan
   d. All the above

4. An investigation and assessment of the various adverse events that can affect the organization, conducted as a preliminary phase of the contingency planning process, which includes a determination of how critical a system or set of information is to the organization's core processes and recovery priorities is known as:
   a. Risk assessment
   b. Business impact analysis
   c. Crisis management
   d. Incident damage assessment

5. The process that prepares an organization to reestablish or relocate critical business operations during a disaster that affects operations at the primary site is known as:
   a. Business continuity planning
   b. Disaster recovery planning
   c. Strategic Planning
   d. Operational planning

6. Which level of Organizational Planning typically addresses day-to-day activities and tasks?
   a. Strategic Planning
   b. Tactical Planning
   c. Operational Planning
   d. Top Management Planning

7. The job function of the Chief Information Security Officer includes:
   a. Creating a strategic information security plan with a vision for the future of information security.
   b. Understanding fundamental business activities performed by the company and suggesting appropriate information security solutions that uniquely protect these activities.
   c. Improving the status of information security by developing action plans, schedules, budgets, status reports and top management communications
   d. All the above

8. What is the unit of analysis in the contingency planning approach?
   a. Business Assets
   b. Risk Assets
   c. Business Processes
   d. Risk Factors

By - Saurav kumar

9. Which of the following is not a possible incident indicator?

a. Presence of unfamiliar files
b. Unusual consumption of computing resources
c. Unusual system crashes
d. Activities at unexpected times

10. What is the purpose of conducting an After Action Review (AAR) in incident response?
a. To review and improve the effectiveness of the DRP
b. To review and improve the effectiveness of the BCP
c. To review and improve the effectiveness of the IRP
d. To notify law enforcement agencies