**DANIEL NGEMI**

**21/07340**

**ASSIGNMENT 2**

**INFORMATION SYESTEMS SECURITY AND CRYPTOGRAPHY**

*a)     As an Information Security Officer recently employed in your organization what cybersecurity controls would you implement and how would you implement the various in respect to the threats/attacks*

As an Information Security Officer, my approach, to setting up cybersecurity measures would involve a strategy aimed at safeguarding the organization from threats and attacks. Here are the key steps and controls I would focus on;

Risk Evaluation; To begin with I would conduct an assessment of risks to pinpoint vulnerabilities and threats. This assessment would guide the prioritization of cybersecurity actions based on the seriousness and likelihood of risks.

Implementation of Technical Measures;

Firewalls and Intrusion Detection Systems (IDS); Deployment of firewalls to filter outgoing network traffic along with IDS for detecting and alerting about threats.

Anti malware Solutions; Ensuring all systems have updated antivirus software for detecting and removing software.

Encryption; Using encryption for securing data at rest and in transit to prevent access to information.

Multi Factor Authentication (MFA); Incorporating MFA as a security layer, for accessing systems and data.

Patch Management; Setting up a regular system update schedule to guard against known vulnerabilities.

Implementation of Administrative Measures;

Security Policies and Procedures; Developing security policies and procedures that encompass all facets of information security. Regularly hold training sessions for staff to educate them on cybersecurity risks and recommended practices.

Enforce access control guidelines to guarantee that users possess only the necessary level of access, for their job responsibilities.

Here are the steps to take for security measures;

1. Secure Entry, to Buildings; Control who can enter the buildings where computer systems are kept to prevent entry.

2. Environmental Safeguards; Use measures like fire protection and temperature control to safeguard equipment and data.

3. Monitoring and Response;

Conduct Routine Security Checks; check for security weaknesses and address them promptly.

Incident Management Plan; Create a plan to handle security incidents quickly and effectively.

How to Implement;

Team Collaboration; Work together with IT, HR and department heads to ensure that cybersecurity aligns with business goals.

Technology Usage; Employ up, to date cybersecurity tools that fit the organizations requirements.

Enhancements; Continuously update security strategies and tools to stay ahead of evolving threats.

*b)     Giving relevant examples and diagrams explain the two classes of Cryptographic algorithms below:*

*i) Public Key Encryption (Also known as Asymmetric Encryption);*

Public Key Encryption involves two keys; a key, which is shared openly and a private key, which is kept confidential. The public key is utilized for encrypting data while the corresponding private key is used for decryption. This approach enables communication even if the public key becomes knowledge. For instance; RSA (Rivest Shamir Adleman) stands out as an utilized public key encryption algorithm. It is frequently utilized for data transmission and digital signatures.

Illustration Explanation; Picture a scenario where Person A encrypts a message using Person Bs key. Only Person Bs private key can decrypt this encrypted message ensuring that only Person B can access the content.

*ii) Private Key Encryption (Also known as Symmetric Encryption);*

In Private Key Encryption the key serves for both encryption and decryption processes. Both the sender and receiver must possess this shared key emphasizing the importance of distribution methods. For example; AES (Advanced Encryption Standard) serves as a prevalent symmetric encryption algorithm employed to safeguard data. Recognized for its speed and robust security features AES finds application, in instances such, as file encryption, email security and secure transactions. In this illustration imagine Person A encrypting a message, with a key and sending it to Person B. Person B uses the key to decrypt the message. It's crucial for Person A and Person B to securely share the key, between them.

*c) List the THREE MAJOR Types of information security policy*

1. Organizational (or Master) Security Policy (OSP);

This policy offers an overview of how the company approaches security linking security goals to business objectives and outlining the extent of the information security program.

2. Specific Security Policies (SSP);

These policies focus on aspects of security outlining the rules, guidelines and steps, for implementing security measures. Examples include policies on access control, acceptable use and incident response.

3. System Policies;

These are guidelines that pertain to specific systems or technologies within the organization. They may cover email systems, network infrastructure or procedures, for classifying and managing data.