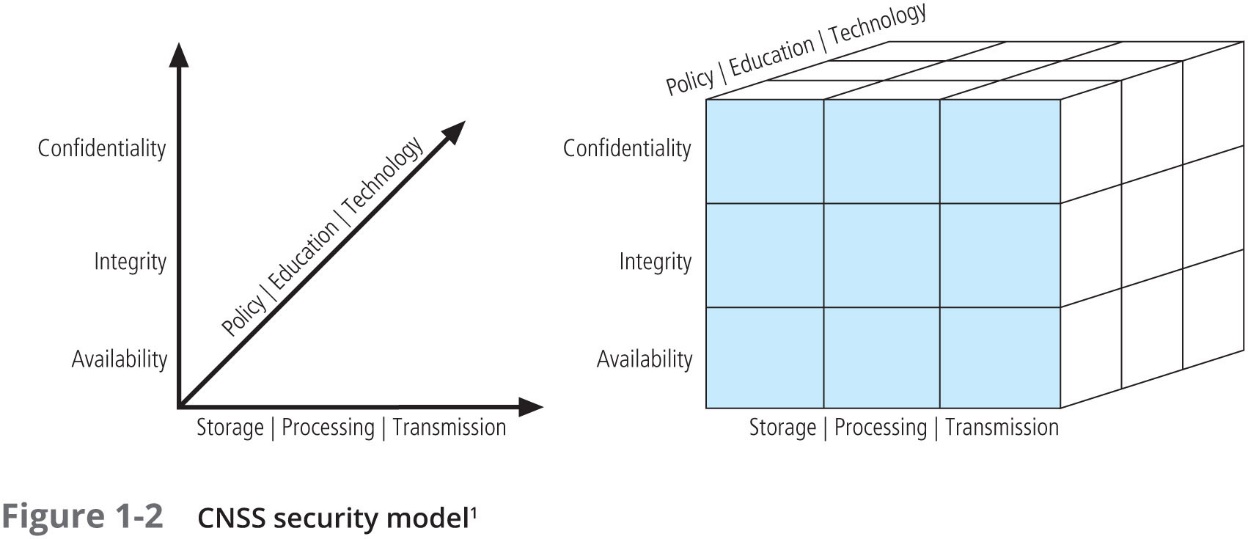
**COMP718 Sem 1 2024**

**LAB week 1 (Introduction to Information Security)**

1. **Content Review**
2. Describe the CNSS security model. What are its three dimensions?



The CNSS security model, commonly known as the McCumber Cube, is a conceptual framework that guides the development of secure information systems. It was created by John McCumber in 1991 and is frequently used to comprehend and apply information security procedures holistically. The model is a three-dimensional cube that incorporates three critical components of information security: goals, states of information, and protections. Each factor is critical for a comprehensive approach to information security.

***The Three Dimensions of the CNSS Security Model:***

* **Security Goals:**
  + **Confidentiality:** Ensures that information is accessible only to those authorized to have access. This goal helps protect sensitive information from unauthorized disclosure.
  + **Integrity:** Ensures that information is accurate and complete, and that it has not been improperly modified. Integrity involves maintaining the correctness and trustworthiness of information throughout its lifecycle.
  + **Availability:** Ensures that information and resources are accessible to authorized users when needed. This involves ensuring that systems are operational and accessible, even in the face of errors or attacks.
* **States of Information:**
  + **Storage:** Refers to information that is being stored and is not actively being processed or transmitted. Security measures must ensure that data at rest is protected against unauthorized access and modifications.
  + **Processing:** Involves information that is currently being processed. Security in this state focuses on protecting data that is being used in applications, systems, or being computed in some way.
  + **Transmission:** Pertains to information that is being transmitted across networks. Security measures focus on protecting data that is in transit from interception, interruption, or manipulation.
* **Safeguards (or Security Measures):**
  + **Policy:** These are the rules and guidelines that govern the behavior of a system and its users. Policies define what is allowed and what is prohibited, helping to enforce the desired level of security.
  + **Education:** Involves training and awareness programs for users, administrators, and managers. Education helps individuals understand the importance of security measures and how to implement them effectively.
  + **Technology:** Refers to the hardware, software, and technical controls used to protect information. This includes firewalls, encryption, intrusion detection systems, and other tools that help in enforcing security policies and protecting information.

Each cell in the McCumber Cube symbolizes a distinct component of security that must be handled, with one element from each of the three dimensions. For example, utilizing technical means to ensure the secrecy of data in storage may include encrypting the data at rest. By taking into account each of the 27 combinations (3 dimensions x 3 components each), the CNSS model provides a comprehensive framework for protecting information systems from a wide range of threats and vulnerabilities. This comprehensive approach is critical for building strong security plans that include all areas of information security.

1. Assume that the CNSS model is used to protect information used in your Class Zoom session. Explain how you would address the components represented in each of the 27 cells. For example:

|  |  |  |
| --- | --- | --- |
| Availability | Storage | Policy: All course material needed for the session is loaded at least 30 min before the session starts |
| Education: Users (lecturers) have received the necessary training in how to store course material and are aware of the limitations. |
| Technology: Storage capacity is sufficient for the course requirements |
| Processing | Policy: Adequate computing resources must be allocated to handle the processing needs of the Zoom session without lag or interruption. |
| Education: Educate users on the minimum system requirements and best practices for optimizing device performance during sessions. |
| Technology: Use of robust servers and efficient software that can handle multiple simultaneous connections and video streams. |
| Transmission | Policy: Network connections should be tested before the session. A protocol for quick switching to a backup connection is established. |
| Education: Users are informed about the bandwidth requirements and instructed on how to reduce bandwidth usage if needed (e.g., turning off video when not necessary). |
| Technology: Implementation of reliable and fast internet services, and use of technologies like Quality of Service (QoS) to prioritize video conferencing packets. |

|  |  |  |
| --- | --- | --- |
| Integrity | Storage | Policy: Access to stored course materials is restricted through authentication mechanisms. |
| Education: Training on the importance of securing login credentials and not sharing them. |
| Technology: Use of encryption for stored data and secure access controls. |
| Processing | Policy: All data processed during the session must be done on secure, authenticated devices. |
| Education: Awareness on secure computing practices and avoiding the use of unsecured devices. |
| Technology: Secure platforms and applications that encrypt data during processing. |
| Transmission | Policy: All transmitted data during the Zoom session must be encrypted. |
| Education: Inform users about the risks of using unsecured networks (e.g., public Wi-Fi) for joining sessions. |
| Technology: Use of end-to-end encryption for all communications during the session. |

|  |  |  |
| --- | --- | --- |
| Availability | Storage | Policy: Implement version control and checksums to verify the integrity of stored materials. |
| Education: Educate users on the importance of not altering files without proper authorization. |
| Technology: Use of file integrity monitoring tools. |
| Processing | Policy: Ensure that only authorized software is used to modify any course-related data. |
| Education: Training on the use of authorized software and the risks of unauthorized data modification. |
| Technology: Application controls that restrict data modification functions to authorized users. |
| Transmission | Policy: Implement protocols to verify data integrity post-transmission. |
| Education: Teach users how to verify file integrity after downloading or receiving files. |
| Technology: Use of secure transmission protocols that include integrity checks, such as HTTPS or secure file transfer protocols. |

1. What is management and what is a manager? What roles do managers play as they execute their responsibilities?

* ***Management*** is the process of organizing, leading, and regulating an organization's resources to achieve certain objectives. It entails organizing people's efforts to achieve goals while making efficient and effective use of the resources available. Management entails the use and management of human, financial, technical, and natural resources.
* ***A manager*** is the person in charge of overseeing or managing an organization or a group of employees. They have a position of responsibility inside an organization and are responsible for managing the operations and work of other employees. Managers are responsible for making decisions that enable the organization to accomplish its goals.

Managers typically perform several roles as they execute their responsibilities.

*Henry Mintzberg, a renowned management expert, categorized these roles into three main groups:*

* **Interpersonal Roles:**
  + **Figurehead:** Symbolic head; obliged to perform a number of routine duties of a legal or social nature.
  + **Leader:** Responsible for the motivation and direction of employees.
  + **Liaison:** Maintains a network of outside contacts who provide favors and information.
* **Informational Roles:**
  + **Monitor:** Receives a wide variety of information; serves as the nerve center of internal and external information of the organization.
  + **Disseminator:** Transmits information received from outsiders or from other employees to members of the organization.
  + **Spokesperson:** Transmits information to outsiders on organization's plans, policies, actions, results, etc.
* **Decisional Roles:**
  + **Entrepreneur:** Searches organization and its environment for opportunities and initiates projects to bring about change.
  + **Disturbance Handler:** Responsible for corrective action when organization faces important, unexpected disturbances.
  + **Resource Allocator:** Makes or approves significant organizational decisions.
  + **Negotiator:** Responsible for representing the organization at major negotiations.

1. How are leadership and management similar? How are they different?

* **Similarities:**

Both leadership and management involve influence, working through people, and are concerned with effective goal accomplishment. Both roles are essential for driving organizational success and involve planning, decision-making, problem-solving, and communication.

* **Differences:**

1. **Focus and Function:** *Management* is primarily focused on the administration, maintenance, and execution of existing processes. It emphasizes control, systems, and structures to achieve efficient and predictable results. *Leadership*, on the other hand, focuses on influencing and inspiring people, envisioning future possibilities, and driving changes and innovations.
2. **Approach:** *Managers* tend to follow established procedures and ensure that their team adheres to these guidelines. *Leaders* focus more on motivating and inspiring their team members to achieve the vision of the organization.
3. **Risk and Vision:** *Leaders* are typically more risk-oriented and focus on long-term visions and strategies. *Managers* are generally more risk-averse and concentrate on short-term goals and solving immediate problems.
4. **Relationship with Team:** *Management* often involves a more formal, hierarchical relationship with team members. *Leadership* fosters a more personal and informal connection, aiming to inspire and engage rather than direct.

*In summary, while management and leadership overlap and are both vital to organizational success, they differ in focus, approach, and methods. Effective organizations often require individuals who can both manage and lead, adapting their approach to the needs of the current situation and the long-term objectives of the organization.*