LESSON 1

Fundamentals of Information Systems

Security

Learning outcomes

Upon completing this lesson, you should be able to:

- Define information security
- Describe fundamentals of information security
- Explain the goals of security
- Identify hacker's techniques
- Discuss threats and their sources
- Discuss various types of hazards

1.1. Introduction

The way security of information and other assets has been handled has evolved over time as our society and technology has evolved. Understanding this evolution is important in order to understand how security needs to be approached today.

Early in history, all assets were physical. Important information was also physical, as it was curved into stone and later written on paper. To protect these assets, physical security was used, such as walls, moats, and guards. Most historical leaders did not place sensitive/critical information in any permanent form, which is why there are very few records of alchemy. They also did not discuss it with anyone except their chosen disciples - knowledge was and is power. Maybe this was their best security.

Sun Tzu said, "A secret that is known by more than one is no longer a secret." If the information was transmitted, it usually went by a messenger and usually with a guard. The risk was purely physical, as there was no way to get to the information without physically grasping it. In most cases, if the information was stolen, the original owner of the information was deprived of it.

1.1.1. What is Security?

Security is the protection of assets. Assets include Hardware, Software and Information. There are three main aspects of security:

- Detection
- Prevention
- Reaction

To access, evaluate and choose various security products and needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfy those requirements. This is difficult enough in a centralized data processing environment with the use of LAN and WAN network since the problems are compounded.

The OSI security architecture is useful to managers as a way of organizing the tasks of providing security. Furthermore, because this architecture was developed as an international standard to cater for computers and communication, vendors have developed security features for their products and services that relates to these structured definitions of services and mechanisms. The OSI security architecture provides a useful abstract overview of many concepts. It focuses on security mechanisms, services, threats and attacks that can be defined as follows:

- **Security mechanism:**

It is a process that is designed to detect, prevent or recover from counter security attack.

- **Security service:**

This is a process or communication service that enhances the security of the data processing system and the information transfer of an organization. The services are intended to counter security attacks and to make use of one or more security mechanisms to provide the service.

- **Security threats:**

These are acts or conditions that may result in the compromise of sensitive information; loss of

life; damage, loss, or destruction of property or disruption of mission. A threat is a potential for violation of security which exists when there is a circumstance, capability, action or event that could breach security and cause harm.

It is a possible danger that might exploit vulnerability.

- **Security attack:**

It is any action that compromises the security information owned by an organization. Attacks

are an assault on system security that derives from an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system. It attempts to bypass security control. The attacker could alter, release or deny data.

The following are examples of security attacks:

1. **Modification Attacks:**

   A modification attack is an attempt to modify information that the attacker is not authorized to modify. The attacker may change or delete existing information, or insert new information. Modifying electronic information is easier than modifying information on paper.

2. **Access Attacks:**

An access attack is an attempt to see information that the attacker is not authorized to see.

3. **Snooping** is looking through information files to find something interesting.

4. **Eavesdropping** is when someone listens in on a conversation that they are not part of.

5. **Interception** is an active attack against the information. To access the information on paper, the attacker needs to gain access to that paper.

Good security may prevent an outsider from accessing information on paper, but may not prevent an insider from gaining access. Computer security deals with the prevention and detection of unauthorized actions by users of a computer system.

1.1.2. Features of Computer Security

- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Authentication
- Access Control
- Accountability