Information Security - Module 1 Overview

Module 1: Information Security Concepts (4 hours)

1. Introduction to Information Security Information security is crucial in protecting digital assets from unauthorized access, data breaches, and cyber threats. With the increasing reliance on digital systems for financial transactions, healthcare, communication, and governance, securing information has become a fundamental necessity. A failure in security can lead to severe consequences, including financial loss, identity theft, and national security risks.

2. Computer Security Computer security refers to protecting computing systems from theft, damage, or unauthorized access. It involves safeguarding:

Hardware: Computers, storage devices, network equipment.

Software: Operating systems, applications, security programs.

Data: Personal information, financial records, business documents.

People: Users interacting with the system.

Processes: Security policies and procedures that enforce protection.

3. Vulnerability-Threat-Control Paradigm To understand security threats, three key components must be analyzed:

Vulnerability: A flaw in a system that can be exploited.

Threat: A potential danger that can cause harm.

Control: Security measures that prevent, mitigate, or eliminate vulnerabilities.

Security measures include:

Preventive Controls: Firewalls, antivirus software, access controls.

Detective Controls: Intrusion detection systems, security audits.

Corrective Controls: Incident response plans, recovery mechanisms.

4. Common Threats to Security Threats to security can be categorized as:

Interception: Unauthorized access to data (e.g., eavesdropping, wiretapping).

Interruption: Disrupting system availability (e.g., denial-of-service attacks).

Modification: Altering data without authorization (e.g., file corruption, identity spoofing).

Fabrication: Creating false data or activities (e.g., fake transactions, phishing scams).

5. The C-I-A Triad (Security Triad) Security revolves around three core principles:

Confidentiality: Ensures information is accessed only by authorized users (e.g., encryption, access controls).

Integrity: Ensures data accuracy and prevents unauthorized modifications (e.g., checksums, digital signatures).

Availability: Ensures reliable access to data and services (e.g., redundancy, disaster recovery planning).

Additional security properties include:

Authentication: Verifies the identity of users and systems.

Non-repudiation: Ensures that actions cannot be denied later.

Auditability: Tracks security events for accountability.

6. Malicious Code (Malware) Malware is software designed to disrupt, damage, or gain unauthorized access to systems. Common types include:

Viruses: Self-replicating programs that attach to files.

Worms: Standalone programs that spread across networks.

Trojan Horses: Malicious programs disguised as legitimate software.

Ransomware: Encrypts files and demands payment for decryption.

Spyware: Collects user data without consent.

Security measures include:

Regular software updates and patching.

Using reputable antivirus and anti-malware tools.

Avoiding suspicious downloads and email attachments.

7. Advanced Persistent Threats (APT) APTs are sophisticated cyber-attacks targeting high-value entities such as governments, corporations, and research institutions. Characteristics include:

Long-term infiltration and persistence within the target system.

Use of social engineering tactics to gain access.

Covert data exfiltration without detection.

8. Types of Attackers Cybersecurity threats come from different sources:

Hackers: Individuals exploiting security weaknesses.

Organized Crime: Groups involved in financial fraud, extortion, and data theft.

Terrorists: Entities using cyber means for political disruption.

State-Sponsored Actors: Government-backed groups conducting espionage and cyber warfare.

9. Security Controls and Countermeasures Security measures fall into three categories:

Physical Controls: Locks, surveillance cameras, restricted access.

Technical Controls: Firewalls, encryption, authentication mechanisms.

Administrative Controls: Security policies, compliance regulations, employee training.

10. Risk Management Managing security risks involves:

Identifying vulnerabilities through security assessments.

Evaluating risks based on potential impact and likelihood.

Implementing risk mitigation strategies such as access restrictions, data backups, and security monitoring.

11. Testing and Evaluation Testing security systems ensures they function correctly:

Black-Box Testing: Evaluates system functionality without knowledge of internal workings.

White-Box Testing: Tests system security with full access to internal design.

Regression Testing: Ensures updates do not introduce new vulnerabilities.