**Module - 1 | Security in Computing**

**Computer Security**

* The protection of assets of a computer and/or its components.
* Prevents attacks and use control or countermeasures.

**Security Properties**

* Integrity
* Authentication
* Nonrepudiation/accountability.

**C-I-A Triad**

* **Confidentiality**
  + Ensuring that sensitive information is accessed only by authorized individuals.
* **Integrity**
  + Maintaining the accuracy and reliability of data, ensuring it is not altered or tampered with.
* **Availability**
  + Ensuring that information and resources are accessible to authorized users when needed.

**Characterizations of harm**

* Interception
* Interruption
* Modification

**Threat Options**

* Human/nonhuman
* Malicious/nonmalicious
* Random attacks
* Directed attacks

**Common Vulnerability Scoring System (CVSS)**

* It provides a standard measurement system that allows accurate and consistent scoring of vulnerability impact.

**Attackers**

* Cyberthreats/cyberattackers
  + Individuals
  + Worldwide groups
  + Organized crime
  + Terrorists
* Advanced Persistent Threats (APTs)

**How Terrorists Use Computers**

* Computer as **target** of attack.
* Computer as **method** of attack.
* Computer as **enabler** of attack.
* Computer as **enhancer** of attack.

**Vulnerabilities**

* Weaknesses that can allow harm to occur.
* Weak authentication.
* Lack of access control
* Errors in programs
* Finite or insufficient resources.
* Inadequate physical protection.

**Controls**

* Prevent
* Deter
* Deflect
* Mitigate
* Recover

**Types of Countermeasures**

* Physical controls
  + Locks. Walls/fences, (human) guards, sprinklers, sensors, etc.
* Procedural or administrative controls
  + Laws, regulations, policies, procedures, guidelines, copyrights, patents, contracts, agreements, etc.
* Technical controls
  + Passwords, program or operating system access controls, network protocols, firewalls, intrusion detection systems, encryption, etc.