Lecture-1

What is Information Security

Information Security (InfoSec)

- Refers to the protection of important information against unauthorised access, disclosure, use, modification, or disruption.
- It ensures that sensitive organisational data is available to authorised users, remains confidential, and maintains its integrity.

Key Terms

Unauthorised access

- Access to information or systems by users who do not have permission.

Disclosure

- The exposure or release of sensitive information to unauthorised parties.

Alteration / modification

- Unauthorised changes to information that damage its accuracy or reliability.

Confidential

- Ensuring information is only accessible to those who are authorised to view it.

Integrity

- Keeping information accurate, complete, and free from unauthorised modification.

More About Information Security

IT security

- It is concerned with protecting physical and digital IT assets and data centres but does not include protection for the storage of paper files and other media.
- It focuses on the technology assets rather than the information itself.

Cybersecurity

- It focuses on securing digital information systems.
- The goal is to help protect digital data and assets from cyberthreats.
- It is not concerned with protecting paper or analogue data.

Data security

- It includes the physical security of hardware and storage devices, along with administrative and access controls.
- It also covers the logical security of software applications and organisational policies and procedures.

2. CIA Triad

The **CIA Triad** is the core model of information security:

Confidentiality

- Ensures information is only accessible to authorised users
- Examples:
  - Encryption
  - Access control
  - Authentication

Integrity

- Ensures information is accurate and has not been altered improperly
- Examples:
  - Hashing
  - Checksums
  - Digital signatures

Availability

- Ensures systems and data are accessible when needed
- Examples:
  - Redundancy
  - Backups

- DDoS protection

All three must be balanced — improving one can sometimes weaken another.

---

3. Threats

A **threat** is **anything capable of causing harm** to a system or data.

Examples:

- Hackers
- Malware
- Natural disasters
- Insider misuse
- System failures

---

4. Vulnerabilities

A **vulnerability** is a **weakness** that can be exploited by a threat.

Examples:

- Weak passwords
- Outdated software
- Misconfigured servers
- Poor access control

---

5. Exploits

An **exploit** is a **tool or technique** that takes advantage of a vulnerability.

Examples:

- SQL Injection
- Buffer overflow
- Phishing emails
- Zero-day exploits

---

6. Attacker Types

Different attackers have different motivations:

- **Cyber Criminals**

  → Financial gain (fraud, ransomware)

- **Hacktivists**

  → Political or social motives

- **Insiders**

  → Employees or trusted users abusing access

- **Script Kiddies**

  → Low skill attackers using pre-made tools

---

7. Malware Types

Malware = malicious software designed to harm systems.

- **Virus** – attaches to files and spreads when executed
- **Worm** – self-replicates across networks
- **Trojan** – disguises itself as legitimate software
- **Ransomware** – encrypts data and demands payment
- **Spyware** – secretly collects user data
- **Rootkit** – hides attacker presence and maintains access

---

8. Risk Formation

Security risk forms through a chain:

Threat → Vulnerability → Exploit → Impact

- If any link is removed, risk is reduced
- Organisations manage risk by:
  - Reducing vulnerabilities
  - Blocking exploits
  - Minimising impact