UNIT 1: Understanding Principles of Cyber Security

1.1 The Concepts of Cyber Security

Cyber security is about protecting computers, networks, data, and systems from being attacked, stolen, or damaged.
It involves using technology, processes, and good habits to keep information safe.
The main ideas include:

- **Confidentiality**: keeping data private and only accessible to authorised people.
- **Integrity**: making sure data is not changed or tampered with.
- **Availability**: ensuring systems and information are ready when needed.

Cyber security also includes areas like network protection, secure passwords, encryption, backups, and awareness training.

1.2 The Importance of Cyber Security

Cyber security is important because we use technology in nearly everything such as banking, healthcare, shopping, and education.
Without strong security:

- Businesses could lose money and trust.
- People's personal information could be stolen.
- Services like hospitals or schools could be disrupted.

Good cyber security protects data, reputation, and operations.
It also helps organisations follow laws like GDPR and maintain customer confidence.

1.3 The Consequences and Implications of Inadequate Cyber Security

Economic Costs of Cyber Attacks

Cyber attacks can cost a company millions. They might have to pay for:

- Repairing systems and recovering data.
- Lost income from downtime.
- Ransom payments if hit by ransomware.
- Fines for breaking data protection laws.

Reputational Damage

If customers lose trust, they may stop doing business with the company.
Bad publicity can harm a brand for years even after systems are fixed.

Legal Consequences of Cyber Breaches

If an organisation does not protect data properly, it can face lawsuits or fines under data protection laws such as GDPR.
They might also have to report the breach and prove what went wrong.

2.1 Define Core Terminology Used in Cyber Security

- **Threat**: something that could cause harm such as malware or phishing.
- **Vulnerability**: a weakness in a system that an attacker could exploit.
- **Risk**: the chance of a threat taking advantage of a vulnerability.
- **Exploit**: a tool or method used to attack a weakness.
- **Firewall**: software or hardware that filters network traffic.
- **Encryption**: converting data into code to keep it secret.
- **Malware**: malicious software designed to cause harm.
- **Phishing**: tricking someone into giving away information such as passwords.

2.2 Explain the Terms Good Actors and Bad Actors

Bad Actors

Bad actors are people or groups that try to cause harm through technology.
They might steal data, damage systems, or attack networks for personal gain or disruption.

Examples:

- Hackers, cybercriminals, or hacktivist groups.
- Insiders who misuse access to steal information.

Good Actors

Good actors work to protect systems and data.
They use ethical methods to test, secure, and improve cyber defences.

Examples: Cyber security professionals, ethical hackers, IT admins, and analysts.

2.3 Distinguish Typical Behaviours of Good Actors and Bad Actors

Good Actors	Bad Actors
Protect and defend systems	Attack or exploit systems
Follow laws and policies	Break laws for gain or revenge
Test security safely	Cause harm or disruption
Share knowledge to improve defences	Hide identity and actions

2.4 Explain the Motivations of Good Actors and Bad Actors

- **Good actors** are motivated by protecting data, helping people stay safe online, following laws, and improving system performance.

- **Bad actors** are motivated by money, revenge, politics, curiosity, or showing off their skills.

2.5 Identify Key Sectors That Are Most Vulnerable to a Cyber Attack

Financial Institutions

Banks and payment companies are targeted for money and personal data.

Healthcare

Hospitals and clinics store sensitive patient data, often on old systems, which makes them an easy target.

Educational Institutions

Schools and universities hold student information and often have weaker security.

Retailers

They handle credit card and customer data which hackers find valuable.

Manufacturing

Attackers might want to steal designs or disrupt production.

Utilities

Energy and water companies are critical targets because attacks can disrupt entire communities.

2.6 Compare the Motivations for a Cyber Attack in Key Sectors

Sector	Main Motivation
Financial	Stealing money or account data
Healthcare	Access to medical records for identity theft or resale
Education	Data theft or ransom for quick payment
Retail	Stealing card data or customer info
Manufacturing	Industrial spying or disruption
Utilities	Political, sabotage, or terrorism motivations

2.7 Consider How an Actor May Carry Out a Cyber Attack

A bad actor might:

- Research the target and collect information.
- Find vulnerabilities such as weak passwords or unpatched software.
- Deliver an attack using phishing, malware, or network breach.
- Exploit the system to steal data or encrypt files.
- Cover their tracks by deleting logs or hiding identity.

3.1 Describe the Term Security by Design

Security by design means building security into a system from the start, not adding it later. It is about designing software, networks, and systems with protection already in place.

3.2 Explore the Principles of Security by Design

Establish the Context

Understand what needs protection and what threats exist.

Make Compromise Difficult

Use strong passwords, encryption, and access controls.

Reduce the Attack Surface

Limit the number of ways an attacker can get in.

Make Disruption Difficult

Design systems that can still run if something goes wrong.

Make Breach Detection Easier

Include monitoring and alerts to spot suspicious activity early.

Reduce the Impact of an Attack

Use backups, recovery plans, and network segmentation to limit damage.

3.3 The Consequences of Not Considering Cyber Security During the Design Phase

If security is not built in early:

- Systems are easier to hack.
- Fixing issues later is more expensive.
- Data breaches are more likely.
- The company can lose money, time, and trust.

3.4 The Advantages and Disadvantages of Security by Design

Advantages

- Stronger overall protection.
- Saves money in the long run.
- Easier to meet data protection laws.
- Builds customer trust.

Disadvantages

- Takes more planning time at the start.
- Can cost more during development.
- Needs skilled people to implement properly.