

CYBER SECURITY INTERNSHIP – TASK 1

Understanding Cyber Security Basics & Attack Surface

Cyber Security Overview

- Cyber security works silently to protect users in the digital environment.
- Most online services depend on cyber security to function safely.
- A secure system allows users to trust digital platforms.
- Cyber security reduces risks created by modern technology.
- Without cyber security, digital growth would not be possible.

Confidentiality

- Confidentiality protects personal and sensitive information.
- It ensures data is accessed only by authorized users.
- Loss of confidentiality often leads to identity misuse.
- User trust depends on proper data confidentiality.
- Privacy protection is a key goal of confidentiality.

Integrity

- Integrity ensures information remains accurate.
- Data should not change without permission.
- Small data changes can create major issues.
- Integrity helps maintain reliable records.
- Trusted systems depend on data integrity.

Availability

- Availability ensures systems are accessible when required.
- System downtime affects productivity.
- Reliable access improves user confidence.
- Availability supports continuous operations.
- Stable systems reflect good availability.

Attack Surface

- Attack surface includes all possible entry points.
- More features increase attack opportunities.
- Attackers target weak and exposed areas.
- Reducing exposure improves security.
- Understanding attack surface helps prevention.

Types of Attack Surfaces

- Applications and services create attack paths.
- Human behavior increases security risks.
- Third-party tools expand exposure.
- Misconfigurations create hidden vulnerabilities.
- Attack surfaces change over time.

Common Cyber Attackers

- Different attackers have different motives.
- Financial gain is a common motivation.
- Insider threats are difficult to detect.
- Advanced attackers remain hidden longer.
- Attack methods evolve continuously.

OWASP Top 10

- OWASP lists common web security risks.
- Many attacks exploit known weaknesses.
- OWASP improves security awareness.
- Following OWASP reduces common errors.
- It provides practical security guidance.

Data Flow & Attack Points

- Data passes through multiple systems.

- Each stage introduces potential risk.
- Attackers exploit weak validation.
- All layers must be secured.
- Data protection must be continuous.

Importance of Understanding Attack Surface

- Awareness reduces unexpected threats.
- Early detection prevents major damage.
- Security planning becomes more effective.
- Risk management improves with understanding.
- Prevention is easier than recovery.