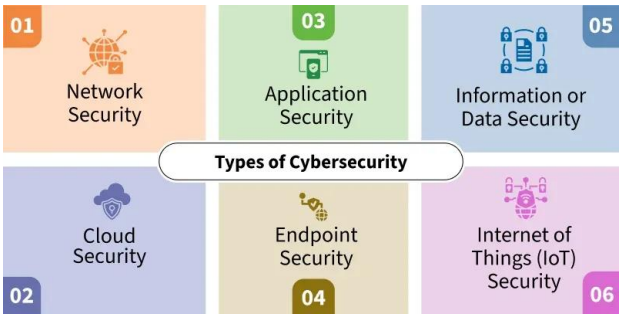
Task 1: Understanding Cyber Security Basics & Attack Surface

Introduction to Cyber Security

Cyber security is the practice of protecting systems, networks, and data from digital attacks. These attacks aim to access, steal, change, or destroy sensitive information. With the increasing use of the internet, cyber security has become essential for individuals, businesses, and governments. Cyber security ensures that digital data remains safe while being stored, processed, and transmitted.



What is the CIA Triad?

The CIA Triad is a model designed to guide information and network security policies within an organization. The three components of the triad—Confidentiality, Integrity, and Availability—are the essential objectives that organizations must prioritize when designing, implementing, and managing security systems, networks, and policies.

a) Confidentiality:- It ensures that information is accessible only to authorized users.

Examples:

- Password protection in email accounts
- OTP verification in banking apps
- Private messages on WhatsApp

Threats: Data leaks, hacking, unauthorized access

b) Integrity:- It ensures that data is accurate and not altered without permission.

Examples:

- Bank transaction records
- Exam result databases
- Medical reports

Threats: Data modification, malware attacks

c) Availability:- It ensures that systems and data are accessible when needed.

Examples:

- Online banking services
- Hospital management systems
- Government websites

Threats: Server failures, DDoS attacks, power outages

These objectives work together to form a comprehensive approach to securing information systems, ensuring that data is protected from unauthorized access, unintentional or malicious alterations, and disruptions that could lead to downtime.

Applications of CIA Triad

Confidentiality is crucial in sectors like healthcare. For example, hospitals use encryption to protect patient records, ensuring only authorized personnel can access sensitive information. This practice not only protects privacy but also complies with regulations like HIPAA.

Integrity plays a vital role in financial institutions. Banks implement hashing algorithms to verify transactions, which prevents unauthorized changes. Without these measures, customers could face significant losses due to manipulated data.

Availability becomes essential during high-demand periods, such as online sales events. E-commerce platforms employ load balancing techniques to distribute traffic across multiple servers. This ensures that customers can access the site without interruptions and complete their purchases smoothly.

Organizations frequently conduct regular audits to maintain all three aspects of the CIA triad effectively. These audits help identify vulnerabilities that could compromise confidentiality, integrity, or availability. In cloud services, providers often use multi-factor authentication for confidentiality, real-time monitoring tools for integrity, and disaster recovery plans for availability. Such practices enhance security while maintaining user trust and operational efficiency.

Ultimately, effective implementation of the CIA triad fosters a secure environment across various industries while protecting against evolving cyber threats.

Different types of attackers

The cyber threat landscape is the different kinds of people and methods that try to harm computers, data, or networks. Knowing who they are and how they attack helps us defend better.

1. Cybercriminals (money-motivated)

People or groups who hack to steal money or sell data.
What they do:

- Ransomware: lock files and demand money.
- Theft: steal data, credit cards, or login details.
- Scams: fake invoices, fraud, Business Email Compromise (BEC).
- Many run-like businesses (e.g., Ransomware-as-a-Service).

2. Script Kiddies (beginners)

Amateur hackers who use ready-made tools and scripts.
Key points:

- They don’t write their own exploits.
- Motivated by fun, attention, or revenge.
- Can cause trouble: DDoS, malware spread, website defacement.

3. Hacktivists (political/ideological)

Hackers who attack for a cause (political, social, environmental).
They may:

- Take down websites (DDoS).
- Leak data to expose wrongdoing.
- Deface sites with messages or doxing.
- Sometimes cooperate with others or use tools that look criminal.

4. Nation-State Actors (state-sponsored)

Government-backed teams with lots of money and time.
They aim to:

- Spy (steal secrets).
- Sabotage critical systems (energy, transport, healthcare).
- Influence politics or steal technology.
  They use very advanced, patient methods and sometimes AI.

5. Insider Threats (from inside the organization)

People inside a company who cause harm, intentionally or by accident.
Types:

- Malicious insiders who steal or sabotage.
- Colluders who work with outside criminals.
- Accidental insiders who make mistakes (like falling for phishing).
  Insider risk rises during layoffs or big changes.

Common attack surfaces

Email-based

- **Phishing:** trick people into clicking links or giving passwords.
  Stages: research → build trust → exploit → execute.
- **BEC (Business Email Compromise):** fake exec emails to steal money.
- **VEC (Vendor Email Compromise):** fake supplier invoices.

Social engineering (attacking people)

- **Spear phishing:** highly targeted phishing.
- **Pretexting:** fake stories to get info.
- **Baiting:** leaving infected USBs or fake offers.
- **Vishing/Smishing:** phone or SMS scams.
  (Humans are the weakest link — many attacks use emotions like fear or greed.)

Web-based attacks

- **XSS (Cross-site scripting):** run bad code in a user's browser.
- **SQL Injection:** trick a site to reveal its database.
- **Keyloggers:** record keystrokes to steal passwords.
- **SSRF:** make a server request internal systems it shouldn't access.
  Use Web Application Firewalls (WAFs) to help block these.

Supply chain attacks

- Hack software or hardware before it reaches users.
- Compromising a trusted supplier can affect many targets downstream

Daily Application Attack Mapping

Example: Banking Application

- User enters login details
- Data is sent to the server
- Server verifies data with database

Possible Attack Points:

- Login page (phishing, brute force)
- Network transmission (man-in-the-middle)
- Database (SQL injection)

Data Flow Explanation

Data Flow:

User → Application → Server → Database

Attack Possibilities:

- User side: Phishing, weak passwords
- Application side: XSS, insecure input handling
- Server side: Misconfiguration, outdated software
- Database side: Unauthorized access, data leakage

Conclusion

This task helped me understand the basics of cyber security, including the CIA triad, attack surfaces, types of attackers, and OWASP Top 10 vulnerabilities. Cyber security awareness is essential in today's digital world to protect information and systems from threats.