Task 1: Cybersecurity Fundamentals

1. Introduction To Cybersecurity

In the modern digital era, almost every aspect of our daily life relies on technology. Activities such as online banking, social networking, digital communication, E-commerce, and cloud storage have become an essential part of both personal and professional environments. As a result, vast amounts of sensitive information are stored, processed, and transmitted over digital systems.

Cybersecurity refers to the practice of protecting digital systems, networks, applications, and data from unauthorized access, misuse, damaged data/data alterations, or disruption. It ensures that digital information remains secure from cyber threats such as hacking, data breaches, and service disruptions. In simple words, it ensures that the data stays safe, unchanged, and accessible only to authorized users.
Cybersecurity exists to answer three basic questions:

a. Who is allowed to access the data?

b. Can the data be trusted to remain unchanged?

c. Will the system work when users need it?

1.1 WHY CYBERSECURITY IS IMPORTANT?

Without cybersecurity, digital systems become vulnerable to attacks that can lead to financial loss, privacy violations, and service disruptions. Therefore, cybersecurity is not only a technical requirement but also a critical necessity for maintaining trust, privacy, and operational continuity in today's digital world.

For example:

a. If a banking system is not secure, attackers could steal money or personal financial details.

b. If social media platforms lack security, private messages and personal information could be exposed.

c. If critical systems become unavailable, essential services such as payments, communication, or healthcare may be disrupted.

Cybersecurity helps prevent these risks by ensuring that digital systems operate safely and reliably.

1.2 Cybersecurity in Everyday Life (Real-World Examples)

Cybersecurity is not limited to large organizations or technical environments; it affects individuals in day-to-day life.

a. Online Banking and Digital Payments

- Cybersecurity protects user accounts through passwords, OTPs, and encryption.
- It ensures that transactions are completed securely and balances are not altered.

b. Social Media and Messaging Applications

- Security mechanisms prevent unauthorized access to user accounts.
- Encryption ensures that private messages remain confidential.

c. Educational and Organizational Systems

- Student records, employee data, and official documents are protected from unauthorized modification or access.
- Secure systems maintain trust and accuracy of information.

1.3 Foundation of Cybersecurity

All cybersecurity practices are built upon a set of core principles that guide how systems are secured and evaluated. These principles are collectively known as the **CIA Triad**, which forms the foundation of cybersecurity decision-making.

The CIA Triad focuses on:

- Protecting sensitive information

- Ensuring accuracy of data
- Maintaining system availability

1.3.1 The CIA Triad - Core Principles of Cybersecurity:

What is the CIA Triad?

The **CIA Triad** is a fundamental cybersecurity model that defines the **three essential goals of information security**. It is used as a decision-making framework to evaluate risks, design systems, and prioritize security controls. Whenever a security decision is made, it is assessed against Confidentiality, Integrity, and Availability.

The CIA Triad stands for:

- **Confidentiality** – Who can access the data
- **Integrity** – Whether the data is accurate and trustworthy
- **Availability** – Whether the system works when needed

In simple terms:

- ***The CIA Triad ensures that data is protected, accurate, and accessible.***

If even one of these principles fails, the security of the entire system is compromised.

1.3.2 Confidentiality

Confidentiality is maintained by ensuring that only **authorized users** can access specific data. This is achieved through **access privilege levels,** where users are given permissions based on what they are allowed to view or do.

Examples:

a. Banking systems: Only the account holder can view balances and transaction history using login credentials and OTPs.

b. social media: Private messages and personal photos are protected through authentication and encryption.

If confidentiality is compromised:

- Sensitive information may be leaked

- Identity theft and financial fraud may occur
  Case example: One of the most impactful cybersecurity incidents in financial systems was the 2014 JPMorgan Chase data breach, where attackers accessed customer record data for over 83 million accounts. Although financial accounts were not directly stolen, exposure of personal information highlighted how breaches can compromise confidentiality in large banking systems.
  (https://en.wikipedia.org/wiki/2014_JPMorgan_Chase_data_breach)

1.3.3 Integrity

Integrity ensures that data remains **accurate, complete, and unaltered** unless modified by an authorized entity.

Simple explanation:

- *Data should not be changed without permission.*

Examples:

- **Banking transactions:** Transaction amounts must remain correct and unchanged during processing.
- **Educational systems:** Student records and marks should not be modified by unauthorized users.

If integrity is compromised:

- Records may be manipulated
- Trust in the system is lost and potential reputational and financial damage

1.3.4 Availability

Availability ensures that systems, applications, and data are **accessible to authorized users whenever required**.

Simple explanation:

- *Security also means that systems should work when users need them.*

Examples:

- **Online banking and UPI:** Services must remain available during peak usage times.
- **Government or university portals:** Websites should function properly during deadlines.

If availability is compromised:

- Services may crash or become unreachable
- Users may face financial or operational losses

Table: 1.3.1 CIA Triad – Core principles

Principle	**Definition**	**Examples**	**What Happens if it is compromised**
Confidentiality	Only authorized users can access data	Bank account protected by password & OTP	Data leaks, identity theft
Integrity	Data remains accurate and unchanged	Correct transaction records in banking	Manipulated or false data
Availability	Systems are accessible when needed	UPI apps working during peak hours	Service downtime, losses

1.4 Why the CIA Triad is Important

The CIA Triad serves as the **foundation of cybersecurity decision-making**. Security controls, policies, and technologies are designed to balance all three principles simultaneously.

For example:

- Strong confidentiality without availability may make systems unusable.
- High availability without integrity may spread incorrect data.
- Integrity without confidentiality may expose sensitive information.

Therefore, an effective cybersecurity strategy must ensure **confidentiality, integrity, and availability together**.

2. Cyber Attackers and Threat Actors

2.1 What is a Cyber Threat?

A **cyber threat** is **a potential action, event, or actor that can compromise the security of digital systems or data**.

Examples of threats include:

- Unauthorized access to accounts
- Theft of personal or financial data
- Disruption of online services
- Manipulation or deletion of data

A threat does not always mean an attack has already happened — it refers to the **risk or possibility** of harm.

2.2 Who are Cyber Attackers / Threat Actors?

A **cyber attacker**, also known as a **threat actor**, is **a person or group that carries out cyber-attacks** or attempts to exploit digital systems (by exploiting security vulnerabilities/weaknesses).
Insider threats are particularly risky because insiders already have valid access privileges, which can be misused intentionally or unintentionally.

They may attack systems:

- Intentionally or unintentionally
- For profit, curiosity, ideology, or national interests
- Using simple tools or advanced techniques

In cybersecurity, the terms **"cyber attacker"** and **"threat actor"** are often used interchangeably in industry and research.

2.3 How Are Threat Actors Classified?

Threat actors are commonly classified based on:

- **Intent** (why they attack)
- **Skill level** (how advanced they are)
- **Access level** (external or internal)
- **Scale of impact** (individual vs organized groups)

This classification helps security teams:

- Understand risks
- Prioritize defenses
- Design appropriate security controls

2.4 Common types of Cyber Attackers:

Attacker Type	**Who They Are**	**Main Purpose**	**Typical Targets / Actions**
Script Kiddies	Beginners using existing tools	Curiosity, experimentation	Weak websites, basic systems
Cybercriminals	Individuals or groups committing online crimes	Financial gain	Banking systems, users
Insider Threats	People with authorized access	Misuse of access (intentional or accidental)	Company data, internal systems
Hacktivists	Ideology-driven attackers	Political or social impact	Government or corporate sites
Nation-State Actors	Government-backed groups (Government-sponsored)	Espionage or disruption	Critical infrastructure
APT Groups	Long-term, stealthy attackers	Data theft, surveillance	Enterprises, governments

Attacker Type	Who They Are	Main Purpose	Typical Targets / Actions
Phishers	Social engineering attackers	Stealing credentials	Emails, fake websites
Malware Developers	Creators of malicious software	Enable cyber attacks	Systems, networks
Botnet Operators	Controllers of infected devices	Large-scale attacks	Websites, services
Ransomware Groups	Extortion-focused attackers	Financial profit	Organizations, hospitals
Corporate Spies	Business-focused attackers	Competitive advantage	Trade secrets
Cyber Terrorists	Disruption-focused attackers	Fear and instability	Public infrastructure
Opportunistic Attackers	Attack any exposed system	Easy exploitation	Unpatched systems
Fraudsters	Scammers using digital platforms	Financial deception	End users
Data Brokers (Illegal)	Sellers of stolen data	Profit from breaches	Personal databases

2.5 Why Understanding Threat Actors Matters

Understanding threat actors helps organizations:

- Predict attack patterns
- Strengthen weak points
- Train users effectively
- Apply the right security controls

Different attackers pose different risks, and not all threats require the same defensive approach.

3. Attack Surfaces and Vulnerabilities

3.1 What is an Attack Surface?

An attack surface refers to all the possible points where an attacker can interact with or attempt to exploit a system. As the system grows in features, connections, users, and technologies, its attack surface also increases.

3.2 What is a Vulnerability?

A **vulnerability** is a **weakness or flaw** in a system, application, or process that can be exploited by an attacker.

Examples of vulnerabilities:

- Weak passwords
- Software bugs
- Misconfigured servers
- Poor access controls

→ **Attack Surface = Where attackers attack**

→ **Vulnerability = How attackers succeed**

3.2.1 What is risk?

Risk refers to the likelihood and potential impact of a threat exploiting a vulnerability.

→ *In cybersecurity, risk exists when a threat can exploit a vulnerability.*

Risk = Threat × Vulnerability

- If there is a threat but no vulnerability, the system is less likely to be compromised.

- If there is a vulnerability but no threat, the risk remains low.

Risk = Threat × Vulnerability × Impact

3.3 Common Attack Surfaces in Modern Systems

Modern digital systems expose multiple points where attackers can attempt to gain access. These points are known as **attack surfaces**. Understanding them helps organizations identify where security controls are most critical.

The table below summarizes the **most common attack surfaces**, their purpose, typical vulnerabilities, and why they are risky.

Attack Surface	What It Includes	Typical Vulnerabilities	Why It Is Risky
Web Applications	Websites, login pages, dashboards, forms	Poor input validation, weak authentication, insecure file uploads	Available to the public and easily accessible/targeted by attackers
Mobile Applications	Android/iOS apps, local storage, permissions	Insecure local storage, weak authentication, improper permission handling	Store sensitive user data on personal devices
APIs	Backend services, endpoints, data exchange interfaces	Broken access control, exposed endpoints, lack of rate limiting	Often expose direct access to data and logic
Network Infrastructure	Routers, switches, servers, ports, protocols	Open ports, weak configurations, unencrypted traffic	Allows attackers to intercept or move laterally
Cloud Infrastructure	Cloud servers, storage buckets, databases	Misconfigured permissions, public storage exposure	Misconfigurations can expose massive data
Databases	User data, credentials, transaction records	Weak access controls, SQL injection	Direct access to sensitive information
Authentication Systems	Login systems, session handling, identity services	Weak passwords, session hijacking	Enables account takeover

Attack Surface	What It Includes	Typical Vulnerabilities	Why It Is Risky
Email Systems	Email servers, clients, attachments	Phishing, malicious links, malware attachments	Primary entry point for social engineering
IoT Devices	Smart devices, sensors, cameras	Default credentials, lack of updates	Often poorly secured and widely deployed
Third-Party Services	External APIs, vendors, integrations	Supply chain vulnerabilities	Attacks spread through trusted connections

3.4 Why Vulnerabilities Are Dangerous

Vulnerabilities are dangerous because they:

- Allow unauthorized access
- Enable data theft or manipulation
- Can disrupt services
- Reduce trust in systems

If vulnerabilities are not identified and fixed, attackers can exploit them repeatedly.

3.5 OWASP Top 10: 2025 – Critical Web Application Security Risks

The **OWASP Top 10: 2025** is a globally recognized awareness document that highlights the **most critical security risks affecting modern web applications**.
It reflects **current attack trends, real-world breach data, and evolving technologies**.

The table below explains each risk focusing on **why it matters**.

ID	Risk Name	What It Means	Why It Is Dangerous
A01	Broken Access Control	Users can access data or actions they should not be allowed to	Leads to data leaks, privilege escalation

ID	Risk Name	What It Means	Why It Is Dangerous
A02	Security Misconfiguration	Systems are set up insecurely or left with default settings	Exposes systems to easy attacks
A03	Software Supply Chain Failures	Vulnerabilities in third-party libraries or dependencies	Attacks spread through trusted software
A04	Cryptographic Failures	Weak or missing encryption for sensitive data	Confidential data can be exposed
A05	Injection	Malicious input is sent to the application	Attackers can manipulate databases or systems
A06	Insecure Design	Security not considered during application design	Flaws exist even if code is correct
A07	Authentication Failures	Weak login, session, or identity management	Accounts can be hijacked
A08	Software or Data Integrity Failures	Data or updates are not verified for integrity	Malicious code or data tampering
A09	Security Logging and Alerting Failures	Attacks are not logged or detected properly	Breaches go unnoticed for long periods
A10	Mishandling of Exceptional Conditions	Errors and edge cases are not handled safely	Leads to crashes, data leaks, or bypasses

Table 3.5: *This section is based on the official OWASP Top 10: 2025 release, which reflects the latest application security risks and industry trends.*

3.6 Why OWASP Top 10 Matters

The OWASP Top 10 helps organizations:

- Identify **high-risk vulnerabilities**
- Prioritize security efforts

- Build secure applications by design
- Improve developer and user awareness

It is widely used by:

- Security professionals
- Developers
- Organizations
- Academic institutions

3.7 OWASP Top 10 and Attack Surfaces (Connection)

- Attack surfaces expose **where attackers can interact**
- OWASP vulnerabilities explain **how those interactions become dangerous**

Together, they form the foundation of **modern application security assessment**.

4. Mapping Daily-Use Applications to Attack Surfaces

Modern applications interact with users through multiple layers, which exposes them to **different attack surfaces**. Understanding this mapping helps identify **where security risks may arise** in everyday digital activities.

4.1 Email Applications (e.g., Gmail, Outlook)

Key Characteristics:

- Used for communication
- Handles sensitive personal and business data
- Accessible via web and mobile

Application Component	Attack Surface	Possible Risk
Login Page	Web Application	Credential theft, brute force
Email Attachments	User Interface	Malware delivery
Email Links	Social Engineering	Phishing attacks
Mail Servers	Network Infrastructure	Unauthorized access
Cloud Mail Storage	Cloud Infrastructure	Data exposure

4.2 Messaging Applications (e.g., WhatsApp)

Key Characteristics:

- Mobile-first application
- Real-time communication
- Stores messages and media

Application Component	Attack Surface	Possible Risk
Mobile App Interface	Mobile Application	Reverse engineering
Message Transmission	Network	Interception if insecure
Media File Handling	Application Logic	Malicious file exploitation
APIs for Messaging	APIs	Broken access control
Cloud Backups	Cloud Infrastructure	Unauthorized data access

4.3 Online Banking Applications

Key Characteristics:

- Handles financial transactions
- Requires strong authentication
- Highly sensitive data

Application Component	Attack Surface	Possible Risk
User Login	Web / Mobile Application	Account takeover
Transaction Processing	Application Logic	Transaction manipulation
Backend APIs	APIs	Unauthorized fund access
Network Communication	Network	Man-in-the-middle attacks
Banking Databases	Cloud / Server Infrastructure	Data breaches

4.4 Why This Mapping Is Important

Mapping applications to attack surfaces helps:

- Understand real-world risks
- Identify weak points in systems

- Improve user awareness
- Strengthen security controls

Even applications we trust daily rely on **multiple interconnected components**, each of which must be secured.

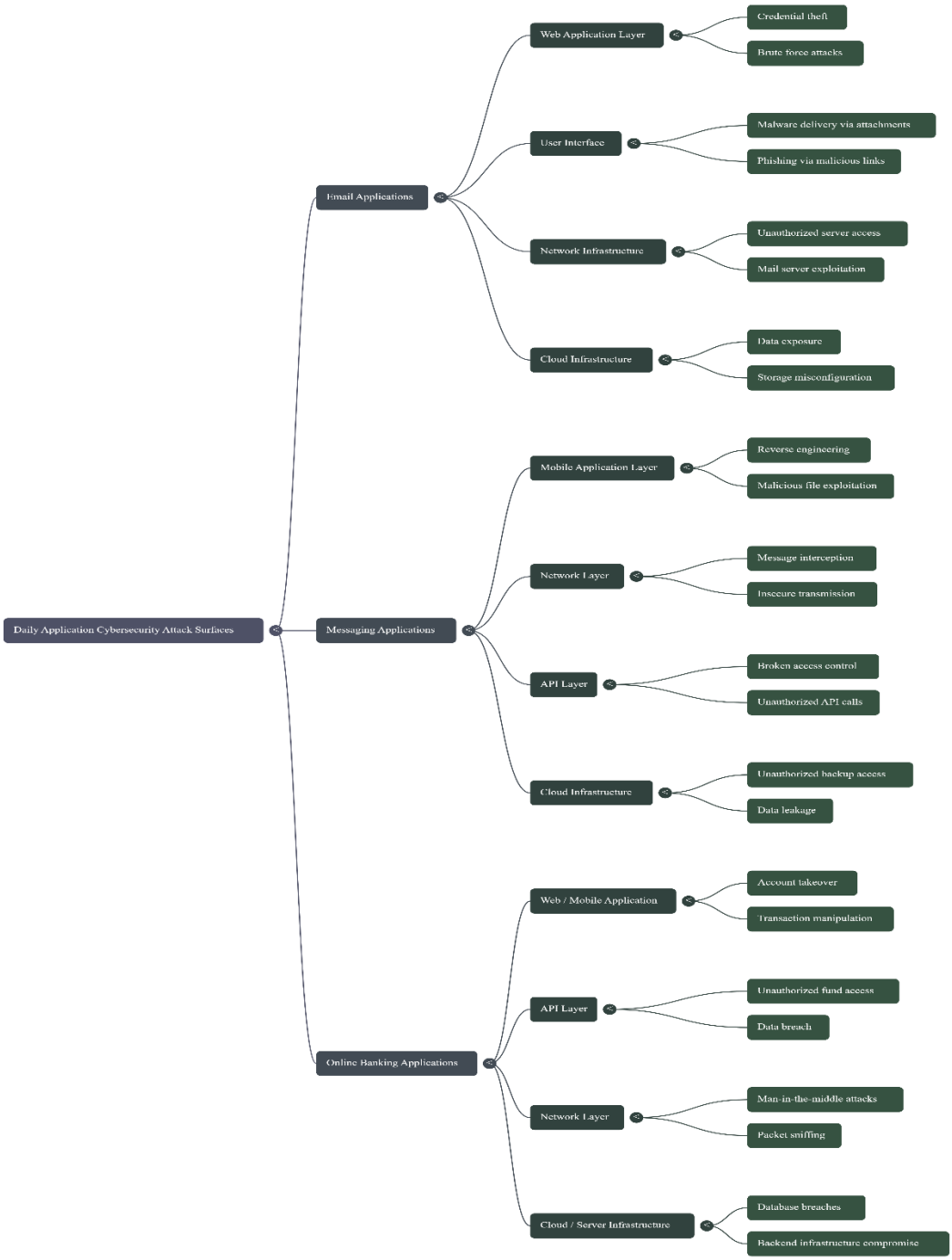


Figure 1*: Mapping of Daily-Use Applications to cybersecurity attack surfaces.*

This mind map illustrates how everyday applications such as email, messaging, and online banking interact with multiple attack surfaces, highlighting potential security risks across different system layers.

5. Data Flow in Applications and Security Risks

5.1 Basic Data Flow in a Typical Application

In most modern applications, data flows through the following stages:

User → Application → Server → Database → Server → Application → User

Each stage in this flow represents a point where data is either **in transit** or **at rest**, and both can be targeted by attackers.

5.2 Step-by-Step Data Flow Explanation:

Layer / Stage	What Happens at This Stage	Data State	Possible Security Risks
User Layer	The user enters data such as login credentials, messages, or transaction details through the application interface.	Input data	Phishing, malicious input, social engineering
Client Application Layer	The web or mobile application receives the input, performs basic validation, and prepares requests to send to the server.	Data in transit	Client-side manipulation, insecure input validation
Application Server Layer	The server processes requests, applies business logic, authenticates users, and enforces authorization rules.	Data in processing	Broken access control, authentication failures
Server–Database Interaction	The server communicates with the database to store or retrieve required information.	Data in transit	Injection attacks, unauthorized queries

Layer / Stage	What Happens at This Stage	Data State	Possible Security Risks
Database Layer	Sensitive information such as user data, messages, or transactions is stored and managed.	Data at rest	Data breaches, unauthorized data access
Response Flow (Back to User)	The processed response travels back from the database through the server and application to the user.	Output data	Information leakage, improper error handling

5.3 Where Attacks Can Occur in the Data Flow

The table below maps each stage of the data flow to **possible attack scenarios**

Data Flow Stage	What Happens Here	Possible Attacks
User → Application	User submits data	Phishing, malicious input
Application Layer	Input handling & validation	Injection, insecure design
Application → Server	Data sent over network	Man-in-the-middle attacks
Server Layer	Authentication & logic	Broken access control
Server → Database	Queries sent to database	Injection attacks
Database	Data storage	Data breaches
Database → Server	Data retrieval	Unauthorized data access
Server → Application	Response processing	Data manipulation
Application → User	Data displayed to user	Information leakage

5.4 Security Insight

a. Data in transit must be protected using secure communication**.**

b. Data at rest must be protected using access control and encryption

c. Weakness at any single stage can compromise the entire system

5.5 Key Takeaway

Cybersecurity is not about securing one component, but about protecting **the entire data flow** from input to storage and back to the user.

Data Flow and Attack Points – (Explained Through the Diagram)

a. Data starts with the **user**, who provides inputs such as login credentials, messages, or transaction details.

b. The **client application (web/mobile)** receives this input and prepares it for processing, making it a common target for malicious inputs and client-side manipulation.

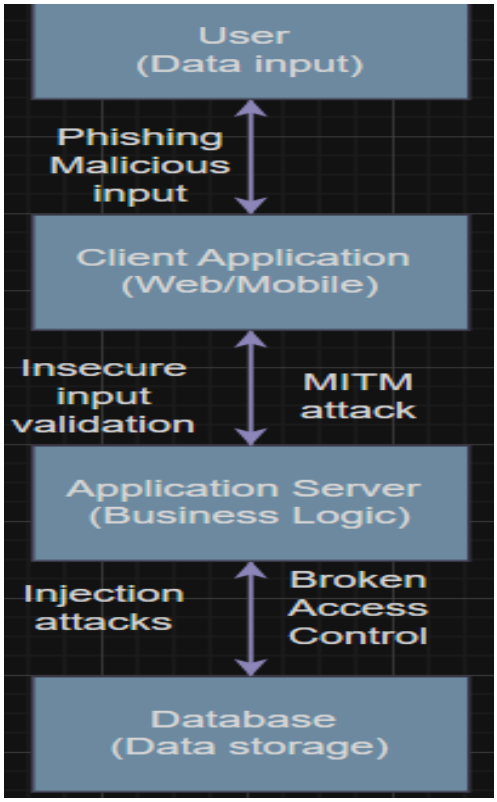
c. Data is then transmitted from the client application to the **application server**, where authentication, authorization, and business logic are applied.

d. During this transmission, attackers may attempt **man-in-the-middle attacks** to intercept or modify data in transit.

e. The **application server** communicates with the **database** to store or retrieve sensitive information.

f. At the server and database level, vulnerabilities such as **injection attacks** or **broken access control** can lead to unauthorized data access.

g. The processed response travels back through the same path to the user, where improper handling can result in **information leakage**.



This flow shows that security must be enforced at **every layer**, as an attack at any point can compromise the entire system.

Final summary / Conclusion:

Through this task, I developed a clear understanding of how cybersecurity works as a connected system rather than a set of isolated concepts. Cybersecurity is not only about preventing attacks, but also about ensuring that data remains confidential, unaltered, and accessible when required, which is represented by the CIA Triad.

Learning about different attackers made it clear that security risks are not limited to external attackers alone. Security risks can originate from various sources, including insiders with legitimate access. This highlighted the importance of understanding attacker intent and access privilege levels when assessing security risks.

Learning about attack surfaces and vulnerabilities helped me understand where systems are most exposed and how weaknesses can be exploited. Modern applications rely on multiple components such as web interfaces, mobile applications, APIs, networks, and cloud infrastructures, each of which introduces potential points of attack. The OWASP top 10 further reinforced this by showing the most common and critical vulnerabilities found in real-world applications.

Mapping daily-used applications to attack surfaces and analysing data flow between the user, application, server, and database made these concepts more practical. It became clear that attacks can occur at any stage of data flow, whether during user input, data transmission, processing, or storage.

Overall, this task helped me understand that cybersecurity requires securing every layer of an application, that it works as a chain. A single weakness anywhere in the system can compromise the entire flow. Therefore, securing applications requires attention at every layer, rather than focusing on just one component.