REPORT: Cyber Security Basics & Attack Surface Analysis
Intern Name: Vishwajit Shirish Daund
Date: 15/1/2026
Task: Task 1 – Understanding Cyber Security Basics

## 1. Introduction

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. This report analyzes the foundational pillars of security, the actors who threaten them, and the surfaces they attack.

## 2. The CIA Triad: The Core of Security

The CIA Triad is a security model used to guide policies for information security within an organization. It consists of three main components:

- **Confidentiality (Privacy)**
  - **Definition:** Ensuring that sensitive information is accessible only to those authorized to have access.
  - **Real-World Example (Banking):** When a user logs into a banking app, the bank uses **Two-Factor Authentication (2FA)** and **AES-256 Encryption**. This ensures that even if a hacker intercepts the data packets, they cannot read the account balance or transaction history without the private key.
  - **Consequence of Failure:** Identity theft, financial loss, and loss of customer trust.
- **Integrity (Accuracy)**
  - **Definition:** Maintaining the consistency, accuracy, and trustworthiness of data over its entire lifecycle. Data must not be changed in transit or altered by unauthorized people.
  - **Real-World Example (Social Media/Software):** When downloading a software update or an app, a **Checksum (hash value)** is often used. If the hash of the downloaded file does not match the original publisher's hash, it means the file has been tampered with (potentially containing malware).[1]

  - **Consequence of Failure:** Corrupted data, malicious code injection, or incorrect financial records.[2]

- **Availability (Reliability)[3]**

  - **Definition:** Ensuring that information and resour[4]ces are available to authorized users when they need them.

  - **Real-World Example (E-commerce):** Amazon or Flipkart must remain online during a "Big Billion Day" sale. They use **Load Balancers** and redundant servers to prevent a crash.

    - **Consequence of Failure:** Revenue loss (downtime costs money) and reputational damage.

### 3. Threat Landscape: Who are the Attackers?

Understanding the enemy is crucial for defense. We categorize attackers based on motivation and skill level:

- **Script Kiddies:**
    - *Description:* Unskilled attackers who use existing scripts or hacking tools developed by others (e.g., downloading a DDoS tool from a forum).
    - *Motivation:* Thrill-seeking, bragging rights, or minor vandalism.
    - *Risk:* Low individual skill, but dangerous in large numbers.
- **Insiders (The Internal Threat):**
    - *Description:* Current or former employees, contractors, or partners who have authorized access to the network.
    - *Motivation:* Disgruntled employees seeking revenge, financial gain (selling secrets), or simple negligence (accidental data leaks).
    - *Risk:* Very High, as they already bypass perimeter defenses like firewalls.
- **Hacktivists:**
    - *Description:* Groups of criminals who unite to carry out cyber-attacks in support of political, social, or religious causes (e.g., Anonymous).
    - *Motivation:* Promoting an ideology, exposing secrets, or embarrassment of target organizations.
    - *Risk:* Focused attacks that often aim for "Denial of Service" or website defacement.
- **Nation-State Actors (APTs):**
    - *Description:* Highly sophisticated hackers funded by governments. They are often referred to as Advanced Persistent Threats (APTs).
    - *Motivation:* Cyber espionage, theft of intellectual property, military sabotage, or destabilizing other nations.
    - *Risk:* Extremely High; they have unlimited time and budget.

### 4. Attack Surface Analysis

The "Attack Surface" is the sum of all points where an unauthorized user can try to enter data to or extract data from an environment.

- **Web Applications:**
    - *Vulnerabilities:* SQL Injection (SQLi), Cross-Site Scripting (XSS), Broken Authentication.
    - *Why:* Web apps are publicly accessible 24/7, making them the most common target.
- **Mobile Applications:**
    - *Vulnerabilities:* Hardcoded API keys in the app code, insecure data storage (storing passwords in plain text on the phone), and weak server-side controls.

- **APIs (Application Programming Interfaces):**
  - *Vulnerabilities:* Broken Object Level Authorization (BOLA). Attackers manipulate ID numbers in API calls to access other users' data.
- **Cloud Infrastructure:**
  - *Vulnerabilities:* Misconfigured S3 buckets (public storage), weak IAM (Identity and Access Management) roles, and unpatched virtual machines.

## 5. Data Flow & Attack Vector Map

To secure a system, we must understand how data moves. Below is an analysis of a standard transaction flow.

**Scenario:** A user sends money via a Banking App.

### Step 1: User Input (The Source)

- **Action:** User opens the app and types in their password.
- **Potential Attack: Keylogging malware** on the user's phone records the keystrokes before encryption happens.

### Step 2: Transmission (The Network)

- **Action:** The app sends the login request over the internet to the bank's server.
- **Data Flow:** Client App --> Internet (ISP) --> Load Balancer
- **Potential Attack: Man-in-the-Middle (MitM)** attack. If the user is on public Wi-Fi (e.g., Starbucks), an attacker can intercept the traffic if HTTPS is not properly implemented.

### Step 3: Processing (The Server)

- **Action:** The Web Server receives the request and processes the logic.
- **Data Flow:** Load Balancer --> Web Server
- **Potential Attack: Remote Code Execution (RCE)**. If the server software is outdated, an attacker could run malicious commands on the server itself.

### Step 4: Storage (The Database)

- **Action:** The server asks the database, "Does this user exist?"
- **Data Flow:** Web Server --> Database (SQL)
- **Potential Attack: SQL Injection (SQLi)**. An attacker enters malicious code (e.g., ' OR 1=1 --) into the login field to trick the database into logging them in without a password.

6. Summary & Conclusion

Ultimately, cybersecurity isn't a one-time fix; it's an ongoing commitment to monitoring and getting better. The foundational goal remains the same: use the CIA triad—Confidentiality, Integrity, and Availability—to keep our data private, accurate, and accessible when needed.

The real challenge today is the sheer speed at which technology evolves. With nearly everything moving to the Cloud and mobile devices, our digital "attack surface" is expanding faster than ever. To keep up, we have to know our opponents. Whether we're facing casual threats from bored script kiddies or sophisticated, strategic attacks from nation-states, understanding their motives helps us focus our defenses where they matter most. The simplest, yet most critical, rule is this: map out exactly how your data moves and lock down every single step, from the moment a user touches the app until the information hits the database.