Day_6: Cyber Security

Date: 20/08/2025

Topics:

1. What is cybersecurity (not just the definition, explore in detail)

   Cybersecurity is the practice of protecting digital devices, networks, and sensitive data from cyber threats such as hacking, malware, and phishing attacks.
   Link: https://www.geeksforgeeks.org/ethical-hacking/what-is-cyber-security/

2. Why is cybersecurity imp

   Cyber Security is important because the government, corporations, and medical organizations, collect military, financial, process, and store unprecedented amounts of data on a computer and other properties like personal information, and this private information exposure could have negative consequences.

   Rising Cyber Threats: How Hackers Exploit Weak Security

   Cyber Attacks can wipe out bank accounts, expose private information, and even lock users out of their own devices unless a ransom is paid. The consequences can be long-lasting, leading to emotional distress and financial instability.

3. Challenges for cybersecurity

   1. **Constantly Evolving Threat Landscape**: Cyber threats are constantly evolving
   2. **Lack of Skilled Professionals**
   3. **Limited Budgets**: Cybersecurity can be expensive
   4. **Insider Threats**: Employees or contractors who have access to sensitive information can intentionally or unintentionally compromise data security.
   5. **Complexity of Technology:** With the rise of cloud computing, IoT, and other technologies, the complexity of IT infrastructure has increased significantly.

4. Cybersecurity trends

   1. Before 2015, basic antivirus, firewalls, and internal IT teams were enough against simple viruses and spam.
   2. Between 2016 and 2023, cyberattacks became more serious, with new threats like ransomware, widespread phishing, DDoS attacks, and huge data breaches.

3. Now in 2025, threats like AI-powered attacks, zero-day exploits, deepfake scams, supply chain attacks, and nation-state cyber warfare are making attacks more complex, automated, and targeted than ever.

   AI & ML in Cybersecurity – Detect threats, predict attacks, block suspicious behavior.

   Ransomware Rise – Backup data, invest in security, avoid ransom traps.

   Cloud Security – Strong authentication, update security protocols.

   IoT Vulnerabilities – Secure & update smart devices regularly.

   Zero Trust Security – Verify every access, inside & outside network.

   Cybersecurity Skills Gap – High demand for skilled professionals.

   Regulatory Compliance – Follow data protection laws, avoid fines.

5. Common Cyberattacks and solutions:

1. Malware (Viruses, Worms, Trojans, Ransomware, Spyware)

- **Attack:** Malicious software that damages systems, steals data, or holds it for ransom.
- **Solutions:**
  - Install updated **antivirus/anti-malware software**
  - Apply **regular security patches & updates**
  - Avoid downloading files from untrusted sources
  - Use **firewalls** and endpoint protection

2. Phishing

- **Attack:** Deceptive emails/messages trick users into revealing sensitive data (passwords, credit cards).
- **Solutions:**
  - Enable **email filters & anti-phishing tools**
  - Train users to **identify suspicious links/emails**
  - Enable **multi-factor authentication (MFA)**

    - Verify links before clicking (hover to preview)

3. Password Attacks (Brute Force, Dictionary, Credential Stuffing)

- **Attack:** Hackers try to guess or crack passwords.
- **Solutions:**
    - Use **strong, unique passwords** with complexity
    - Implement **MFA**
    - Use **password managers**
    - Enable **account lockouts** after failed attempts

4. DDoS (Distributed Denial of Service)

- **Attack:** Overloads a network/server with traffic, causing downtime.
- **Solutions:**
    - Use **CDN & DDoS protection services** (Cloudflare, Akamai)
    - Implement **rate limiting & traffic filtering**
    - Configure **firewall & intrusion prevention systems (IPS)**
    - Have an **incident response plan**

5. Man-in-the-Middle (MITM)

- **Attack:** Attacker intercepts communication between two parties to steal/manipulate data.
- **Solutions:**
    - Use **end-to-end encryption (HTTPS, VPNs, SSL/TLS)**
    - Avoid **public Wi-Fi** or use **secure VPN**
    - Enable **DNS security extensions (DNSSEC)**
    - Implement **secure session management**

6. Drive-by Download

- **Attack:** Malicious code automatically downloads when visiting infected websites.
- **Solutions:**
    - Keep **browsers & plugins updated**
    - Use **pop-up/ad blockers**

  - Deploy **endpoint protection software**
  - Disable auto-downloads where possible

7. Malvertising (Malicious Advertising)

- **Attack:** Hackers inject malware into legitimate online ads.
- **Solutions:**
  - Use **ad blockers**
  - Keep systems **patched & updated**
  - Implement **web filtering solutions**
  - Use **reputable ad networks**

8. Rogue Software (Fake Security Software)

- **Attack:** Fake antivirus/security apps trick users into installing malware.
- **Solutions:**
  - Download software **only from trusted vendors**
  - Educate users on **fake alerts/pop-ups**
  - Use **application whitelisting**
  - Deploy **endpoint detection & response (EDR)**

9. SQL Injection

- **Attack:** Injecting malicious SQL queries into input fields to access databases.
- **Solutions:**
  - Use **prepared statements & parameterized queries**
  - Apply **input validation & sanitization**
  - Restrict **database privileges**
  - Regularly **test with penetration tools**

10. Zero-Day Exploits

- **Attack:** Exploits vulnerabilities before vendors release a fix.
- **Solutions:**
  - Enable **intrusion detection & prevention systems**
  - Apply **virtual patching** via WAF (Web Application Firewall)

    - Monitor systems with **threat intelligence feeds**
    - Keep systems updated as patches are released

11. Insider Threats

- **Attack:** Employees or contractors misuse access for malicious activity.
- **Solutions:**
    - Implement **least privilege access controls**
    - Use **monitoring & auditing tools**
    - Conduct **employee awareness training**
    - Deploy **data loss prevention (DLP) tools**

12. Social Engineering

- **Attack:** Psychological manipulation to trick people into giving access or data.
- **Solutions:**
    - Provide **security awareness training**
    - Verify **identity before sharing sensitive info**
    - Use **strict verification policies**
    - Encourage a **reporting culture**

5. Itam vs csam

ITAM (IT Asset Management)

Focuses on **managing all IT assets** (hardware, software, licenses, cloud resources, etc.)

- Ensures **tracking, lifecycle management, cost optimization** of IT assets
- Covers **procurement → deployment → usage → retirement**
- Helps in **financial control** (reduce costs, avoid overspending)
- Broader scope: includes **hardware, software, cloud, network devices**
- Audience: **IT, Finance, Procurement teams**

CSAM (Cybersecurity Asset Management)

- Focuses on **security visibility and control** of IT/OT/IoT/cloud assets
- Identifies **all assets connected to the network** (including shadow/rogue devices)

- Ensures **continuous monitoring & vulnerability detection**
- Helps in **reducing attack surface** and compliance with security frameworks
- Narrower scope: mainly **security & risk management**
- Audience: **Cybersecurity & Risk teams**

ITAM = “What we own & how we use it” (Inventory + Cost)

CSAM = “What we must secure & protect” (Visibility + Risk)

6. Csam

Cybersecurity asset management (CSAM) is the process created to continuously discover, inventory, monitor, manage and track an organization's assets to determine what those assets do and identify and automatically remediate any gaps in its cybersecurity protections.

If an asset -- be it physical, virtual or cloud-based -- connects to or interacts with other assets on an organization's network, it falls within the scope of CSAM. Examples of assets include the following:

Endpoints – desktops, laptops, mobiles

Network Infrastructure – cloud assets, instances

IoT Devices – sensors & smart gadgets

Appliances – virtual & hardware appliances

Operating Systems – Windows, Linux, etc.

OT Systems – SCADA, HMIs, PLCs

Users – employees, admins, third parties

Physical Infrastructure – buildings, on-prem data centers