Fundamentals of Cyber Security and Threat Landscape

Asst. Prof. Mrs. Priya V. Nagvekar
Computer Science(BCA)
GVMs College

Importance and Challenges in Cyber Security

- Growing digital dependence in all sectors
  - Rapid increase in cyber-attacks and vulnerabilities
  - Shortage of skilled cybersecurity professionals
  - Challenges: evolving threats, zero-day attacks, insider threats
  - Need for continuous monitoring and updated security policies

Importance of Cyber Security

1. Protection of Sensitive Information
    1. Organizations store huge volumes of sensitive data such as:
    2. Personal data (PII), financial details, passwords
    3. Intellectual property (IP)
    4. National security information
    5. Cybersecurity safeguards data from theft, manipulation, or unauthorized access.

Importance of Cyber Security

2. Ensuring Business Continuity
   - Cyber-attacks like ransomware or DDoS can halt business operations.
   - Strong cybersecurity ensures continuous functioning of critical systems and minimizes downtime.

Importance of Cyber Security

3. Protection Against Financial Loss
   - Cyber incidents can cause:
   - Direct financial loss (fraud, ransomware)
   - Indirect loss (reputation damage, legal penalties)
   - Businesses face millions of dollars of economic damage per breach.

Importance of Cyber Security

4. Maintaining Trust and Reputation
   - Customers expect their information to remain private and safe.
   - A security breach can permanently damage an organization’s reputation, causing customer churn and legal consequences.

Cyberspace & Cyber Threat

5. Safeguarding National Security
   - Critical infrastructure like power grids, telecom, water supply, defence systems rely on digital networks.
   - Cybersecurity is essential to prevent nation-state attacks targeting essential systems.

Cyberspace & Cyber Threat

6. Preventing Cybercrime Growth
   - Cybercriminal activities (scams, phishing, identity theft, ransomware, social engineering) are increasing.
   - A robust cybersecurity ecosystem reduces opportunities for attackers.

Cyberspace & Cyber Threat

7. Protection in the Age of IoT & AI
   - Devices such as smart cameras, sensors, medical devices, autonomous vehicles are always connected.
   - Cybersecurity ensures secure communication, avoids privacy leaks, and prevents hijacking of IoT systems.

Cyberspace & Cyber Threat

8. Regulatory Compliance
   - Governments mandate data protection laws (e.g., GDPR, DPDP Act 2023 in India).
   - Cybersecurity ensures compliance, avoiding legal penalties.

Cyber Warfare

- Use of digital attacks by nations to damage or disrupt operations
  - Objectives: espionage, disruption, infrastructure damage
  - Techniques: cyber espionage, sabotage, data theft, misinformation
  - Impact: national security risks and geopolitical tensions

CIA Triad

- Confidentiality: Preventing unauthorized access
  - Integrity: Ensuring data accuracy and trustworthiness
  - Availability: Ensuring systems are accessible when needed
  - Foundation of all cybersecurity policies and practices

Cyber Terrorism

- Use of cyber attacks to create fear and disrupt society
  - Targets: government systems, financial networks, public utilities
  - Motives: political, ideological, or religious
  - Methods: propaganda, defacement, infrastructure attacks

Cyber Security of Critical Infrastructure

- Critical sectors: energy, power grid, transportation, health
  - Risks: nation-state attacks, ransomware, system failures
  - Consequences: large-scale disruption and public safety risks
  - Need for strong monitoring, regulation, and security frameworks