Cyber Security & Cyber Crime – Detailed Comprehensive Guide

Part 1 – Cyber Security

---

1. Introduction to Cyber Security and Its Importance

- **Definition:**
  Cyber security is the discipline of protecting digital systems, networks, applications, and data from unauthorized access, theft, or damage.
- **Why it matters:**
  - **Data protection:** Safeguards personal and business-sensitive data from theft.
  - **Privacy:** Prevents unauthorized monitoring or tracking.
  - **Business continuity:** Reduces downtime from cyber incidents.
  - **Reputation management:** Protects brand image after security breaches.
- **Example:**
  In 2021, Colonial Pipeline's ransomware attack halted fuel supplies, showing how cyber security is essential for infrastructure.

---

2. Cyber Security Frameworks and Standards

Frameworks provide structured guidelines to manage and reduce cyber risks.

1. **NIST Cybersecurity Framework**
   - **Phases:** Identify → Protect → Detect → Respond → Recover
   - **Purpose:** Standardized approach for US organizations to assess risks.
   - **Example:** Used by US federal agencies and critical industries.

2. **ISO/IEC 27001**
    - Focuses on **Information Security Management Systems (ISMS)**.
    - Requires continuous improvement via PDCA (Plan-Do-Check-Act).
    - **Example:** Adopted by multinational corporations for compliance.
3. **COBIT**
    - Focused on **IT governance and control**.
    - Links IT goals with business goals.
    - **Example:** Used in IT audit practices.

Comparison Table:

Framework	Core Focus	Industries Used
NIST	Risk Management	Government, Critical Infrastructure
ISO 27001	ISMS	Corporate, Financial Institutions
COBIT	IT Governance	Auditing, Compliance

---

3. Cyber Security Threats

Threat = Potential cause of an unwanted incident.

- **Malware**
    - Viruses, worms, trojans, spyware
    - **Example:** WannaCry ransomware infected 230,000 computers in 2017.
- **Phishing**
    - Fake emails or websites tricking users into revealing credentials.
- **Ransomware**
    - Encrypts files and demands payment.
- **Man-in-the-Middle (MITM)**
    - Intercepting communication between two systems.

---

4. Cyber Security Vulnerabilities

Vulnerability = Weakness that can be exploited.

- **Technical Vulnerabilities:**
  - **Buffer overflow:** Overwriting memory.
  - **SQL injection:** Injecting malicious queries into databases.
- **Human Vulnerabilities:**
  - Weak passwords.
  - Social engineering.
- **Example:** Equifax breach occurred due to unpatched Apache Struts vulnerability.

---

5. Cyber Security Controls and Countermeasures

Controls are defenses that reduce risk.

- **Technical Controls:**
  - Firewalls, IDS/IPS, antivirus software.
- **Administrative Controls:**
  - Policies, access restrictions.
- **Physical Controls:**
  - Locks, CCTV.
- **Encryption:** AES-256 for storage, RSA for communication.

---

6. Identity and Access Management (IAM)

- **Authentication:** Proving identity (passwords, biometrics, MFA).
- **Authorization:** Defining what a user can do (role-based access).
- **Provisioning:** Adding/removing user accounts.
- **Example:** MFA in Microsoft 365 prevents unauthorized logins.

---

7. Incident Response & Disaster Recovery

- **Incident Response:**
    - Preparation → Detection → Containment → Eradication → Recovery → Lessons Learned.
- **Disaster Recovery:**
    - Backup solutions, failover systems, business continuity planning.

---

8. Cyber Security Awareness and Training

- **Why needed:**
    - 80–90% of breaches involve human error.
- **Training:**
    - Phishing simulations.
    - Strong password workshops.

Part 2 – Cyber Crime

---

1. Introduction to Cyber Crime

- **Definition:**
  Crimes involving computers, networks, or digital devices.
- **Types:**
    - Hacking.
    - Identity theft.
    - Cyberbullying.
    - Fraud.

---

2. Cyber Crime Laws & Regulations

- **India:** IT Act 2000.
- **USA:** CFAA (Computer Fraud and Abuse Act).
- **Europe:** GDPR (focus on data privacy).

---

3. Cyber Crime Investigation & Forensics

- **Steps:**
  - Evidence identification.
  - Collection & preservation.
  - Analysis & reporting.
- **Tools:** EnCase, FTK.

---

4. Cyber Crime Prevention

- Patch management.
- Network monitoring.
- Strong authentication.

---

5. Types of Cyber Attacks

- **DDoS:** Overloading servers with traffic.
- **Phishing:** Deceptive communication.
- **Spear Phishing:** Targeted phishing attack.
- **SQL Injection:** Database manipulation.

---

6. Cyber Terrorism & Warfare

- **Cyber Terrorism:** Attacking public infrastructure.
- **Cyber Warfare:** State-sponsored cyber campaigns.

---

7. Cyber Crime & Digital Evidence

- **Examples:** Metadata, IP logs, deleted files.

---

8. International Cooperation

- INTERPOL.
- CERT collaborations.

Part 3 – Advanced Threats & Countermeasures

---

1. Advanced Persistent Threats (APT)

- Long-term targeted attacks by skilled hackers.
- **Example:** APT29 linked to Russian intelligence.

---

2. Zero-Day Exploits

- Attacks on vulnerabilities before patches are released.

---

3. AI & ML in Cyber Security

- **Uses:** Predictive threat detection, behavior analytics.
- **Example:** Darktrace AI platform.

---

4. IoT Security

- **Risks:** Weak passwords, outdated firmware.
- **Countermeasures:** Device segmentation, strong authentication.

---

5. Cloud Security

- **Risks:** Misconfigured storage, account hijacking.
- **Measures:** Encryption, Zero Trust.

---

6. Blockchain & Crypto Security

- Risks: Exchange hacks, private key theft.
- Security: Multi-sig wallets, cold storage.

---

7. Quantum Computing

- **Risk:** Breaking current encryption.
- **Solution:** Post-quantum cryptography.

---

8. Emerging Technology Security

- **5G:** Network slicing risks.
- **Autonomous Vehicles:** Sensor spoofing prevention.
