

Overview of Cyber Security

Overview of Cyber Security – Study Notes

1. What Is Cyber Security?

Aspect	Description
Definition	Protection of computers, networks, programs, and data from unauthorized access, attack, or damage.
Goal	Preserve confidentiality , integrity , and availability (the CIA triad).
Scope	Includes hardware, software, data, users, processes, and the surrounding environment (cloud, IoT, mobile).

2. Core Principles (CIA Triad)

Principle	Why It Matters	Typical Controls
Confidentiality	Prevents sensitive information from being disclosed to unauthorized parties.	Encryption, access controls, authentication, data classification.
Integrity	Ensures data is accurate, complete, and unaltered.	Checksums, digital signatures, version control, audit logs.
Availability	Guarantees that systems and data are accessible when needed.	Redundancy, load balancing, backups, DDoS mitigation.

3. Major Threat Categories

Threat Type	Examples	Typical Impact
Malware	Viruses, ransomware, spyware, trojans, rootkits	Data loss, system disruption, extortion
Phishing & Social Engineering	Email scams, vishing, pretexting	Credential theft, unauthorized access
Network Attacks	Man-in-the-middle, DDoS, port scanning	Service outage, data interception

Overview of Cyber Security

Threat Type	Examples	Typical Impact
Insider Threats	Malicious employees, accidental leaks	Data exfiltration, sabotage
Vulnerabilities & Exploits	Unpatched software, zero-day bugs	Remote code execution, privilege escalation
Supply Chain Risks	Compromised third-party components	Widespread compromise across multiple organizations

4. Key Defensive Controls

4.1 Preventive Controls

- **Firewalls** – Packet filtering, stateful inspection, next-gen application awareness.
- **Endpoint Protection** – Antivirus, EDR (Endpoint Detection & Response), application whitelisting.
- **Identity & Access Management (IAM)** – Strong passwords, MFA, least-privilege policies.
- **Secure Configuration** – Hardened OS, disabling unnecessary services, baseline standards.

4.2 Detective Controls

- **Intrusion Detection/Prevention Systems (IDS/IPS)** – Signature-based and behavior-based monitoring.
- **Security Information & Event Management (SIEM)** – Centralized log collection, correlation, alerting.
- **Threat Hunting** – Proactive searching for hidden adversary activity.

4.3 Corrective Controls

- **Patch Management** – Timely application of security updates.
 - **Backup & Recovery** – Regular, tested backups; offline/air-gapped copies.
 - **Incident Response (IR)** – Defined playbooks, containment, eradication, post-mortem analysis.
-

Overview of Cyber Security

5. Common Security Frameworks & Standards

Framework / Standard	Focus	Typical Use
NIST CSF (Cybersecurity Framework)	Identify, Protect, Detect, Respond, Recover	U.S. federal agencies, private sector
ISO/IEC 27001	Information Security Management System (ISMS)	International compliance, certification
CIS Controls	20 prioritized actions for defense	Small?to?medium enterprises
PCI DSS	Payment card data protection	Merchants, payment processors

**HIPAA