What Is Cybersecurity?

Definition
Cybersecurity is the practice of protecting systems, networks, and data from digital attacks, unauthorized access, damage, or theft. It spans technologies, processes, and controls designed to safeguard digital assets.

Why It Matters

- **Data Breaches** can expose personal, corporate, or governmental data, leading to financial loss, reputational damage, and legal consequences.
- **Critical Infrastructure** like power grids or hospitals relies on secure networks; attacks can endanger public safety.
- **Business Continuity** ensures services remain available; disruptions (e.g., ransomware) can halt operations.

Key Objectives (the CIA Triad)

1. **Confidentiality** – Ensuring information is accessible only to authorized parties.
2. **Integrity** – Maintaining data accuracy and preventing unauthorized modification.
3. **Availability** – Ensuring systems and data are accessible when needed.

Page 2: Core Concepts & Terminology

1. **Threat**: Any circumstance or event with potential to cause harm (e.g., malware, phishing).
2. **Vulnerability**: A weakness in a system that can be exploited (e.g., unpatched software).
3. **Risk**: The likelihood and impact of a threat exploiting a vulnerability.
4. **Attack Vector**: The path or means by which an attacker gains access (e.g., email, network port).
5. **Exploit**: Code or technique used to take advantage of a vulnerability.
6. **Asset**: Anything of value (data, hardware, software, people).
7. **Control (Safeguard)**: Measure to reduce risk (firewalls, policies, encryption).

Example

- Unpatched web server (vulnerability)
- Internet-facing (attack vector)
- Threat actor exploits it to deface site (attack)
- Data breach exposes customer records (impact)

Page 3: Cybersecurity Domains

Cybersecurity can be subdivided into specialized domains. For a beginner, the key ones are:

1. **Network Security**
    - Protects data moving across networks
    - Tools: firewalls, VPNs, intrusion detection/prevention systems (IDS/IPS)
2. **Endpoint Security**
    - Secures individual devices (PCs, servers, mobile)
    - Tools: antivirus/antimalware, host-based firewalls, EDR (Endpoint Detection & Response)
3. **Application Security**
    - Ensures software is developed and deployed securely
    - Practices: secure coding, code reviews, penetration testing
4. **Data Security**
    - Protects data at rest, in transit, or in use
    - Tools/practices: encryption, data loss prevention (DLP), access controls
5. **Identity & Access Management (IAM)**
    - Manages how users authenticate and gain privileges
    - Technologies: multi-factor authentication (MFA), single sign-on (SSO), role-based access control (RBAC)
6. **Cloud Security**
    - Securing cloud services and infrastructure
    - Shared responsibility model between provider and user

Page 4: Common Threats & Attacks

1. **Malware** (malicious software)
    - Viruses, worms, Trojans, ransomware, spyware
2. **Phishing & Social Engineering**
    - Deceptive emails/websites tricking users into divulging info
3. **Denial-of-Service (DoS/DDoS)**
    - Overwhelming services to render them unavailable
4. **Man-in-the-Middle (MitM)**
    - Intercepting and potentially altering communications
5. **SQL Injection / XSS**
    - Web application attacks inserting malicious code
6. **Zero-Day Exploits**
    - Attacks against previously unknown vulnerabilities
7. **Insider Threats**
    - Malicious or negligent actions by authorized users

Illustration

- Ransomware encrypts files and demands payment.
- Phishing email leads a user to enter credentials on a fake site.
- DDoS flood from a botnet knocks a website offline.

Page 5: Defense in Depth

No single control suffices. Instead, layer multiple defenses:

1. **Perimeter Controls**: Firewalls, network segmentation
2. **Host Controls**: Antivirus, host-based intrusion prevention
3. **Application Controls**: Web application firewalls (WAF), secure SDLC
4. **Data Controls**: Encryption, tokenization
5. **User Controls**: Security awareness training, strong passwords, MFA

Security Layers Diagram (logical)

```
less
CopyEdit
[ User ] ↔ [ Application ] ↔ [ Network ] ↔ [ Host/OS ] ↔ [ Data Storage ]
  |            |                |             |           |
Controls:  Controls:       Controls:       Controls:  Controls:
Training    Input Validation Firewalls      Patching  Encryption
```

Page 6: Risk Management Process

1. **Identify Assets & Threats**
2. **Assess Vulnerabilities & Risks**
3. **Prioritize Risks** (based on likelihood & impact)
4. **Select & Implement Controls**
5. **Monitor & Review**
6. **Repeat (Continuous Improvement)**

Frameworks & Standards

- **NIST Cybersecurity Framework (CSF)**
- **ISO/IEC 27001**
- **CIS Controls**

Page 7: Security Technologies & Tools

Category	Purpose	Examples
Firewall	Block/allow network traffic	Cisco ASA, Palo Alto, iptables
VPN	Secure remote access	OpenVPN, WireGuard
IDS/IPS	Detect/prevent intrusions	Snort, Suricata
SIEM	Aggregate & analyze logs	Splunk, ELK Stack, QRadar
EDR	Endpoint threat detection	CrowdStrike, SentinelOne
Vulnerability Scanners	Find security holes	Nessus, OpenVAS

Category	Purpose	Examples
Penetration Testing	Simulate attacks to find weaknesses	Metasploit, Burp Suite

---

Page 8: Secure Development Lifecycle (SDLC)

1. **Requirements & Planning**: Define security requirements.
2. **Design**: Threat modeling, architecture reviews.
3. **Implementation**: Secure coding practices (e.g., OWASP Top 10).
4. **Testing**: Code reviews, static/dynamic analysis, penetration testing.
5. **Deployment**: Harden configurations, automate secure builds.
6. **Maintenance**: Patch management, incident response planning.

Page 9: Policies, Procedures & Awareness

- **Security Policy**: High-level rules (acceptable use, access).
- **Standard Operating Procedures (SOPs)**: Step-by-step instructions.
- **Incident Response Plan**: Detect, contain, eradicate, recover.
- **Business Continuity & Disaster Recovery (BC/DR)**: Planning for outages.
- **Security Awareness Training**: Phishing simulations, regular updates.

Page 10: Incident Response & Forensics

Incident Response Steps

1. **Preparation**: Tools, communication plan, roles.
2. **Identification**: Detect and validate the incident.
3. **Containment**: Short-term (isolating systems), long-term (hardening).
4. **Eradication**: Remove malware, close vulnerabilities.
5. **Recovery**: Restore systems, monitor for reinfection.
6. **Lessons Learned**: Post-mortem analysis and improvements.

Forensics

- Collect evidence (disk images, logs)
- Maintain chain of custody
- Use forensic tools (Autopsy, FTK)
- Analyze root cause

Page 11: Compliance & Legal Considerations

- **Regulations**: GDPR, HIPAA, PCI DSS, IT Act (India)
- **Data Privacy**: Consent, data classification, retention policies
- **Reporting Obligations**: Breach notification timelines

Example
Under GDPR, organizations must report a personal data breach to authorities within 72 hours.

Page 12: Emerging Trends

- **Zero Trust Architecture**: "Never trust, always verify"
- **Cloud-native Security**: Container security (Docker, Kubernetes)
- **AI/ML in Security**: Anomaly detection, automated threat hunting
- **IoT Security**: Securing smart devices and sensors
- **5G & Edge Computing**: New attack surfaces and low-latency networks

---

Page 13: Best Practices for Beginners

1. **Use Strong, Unique Passwords** & a password manager.
2. **Enable Multi-Factor Authentication (MFA)** everywhere.
3. **Keep Systems & Software Up to Date** (patch promptly).
4. **Back Up Data Regularly** and verify recovery.
5. **Be Wary of Phishing**: Verify senders, don't click unknown links.
6. **Limit Administrative Privileges**: Principle of least privilege.
7. **Encrypt Sensitive Data** at rest and in transit.
8. **Secure Your Home/Office Network**: Change default router passwords, segment IoT.

Page 14: Building Your Skills

- **Online Courses**: Coursera, edX, Cybrary, Udemy
- **Labs & Practice**: TryHackMe, Hack The Box, Cyber Ranges
- **Certifications** (for later):
    - Entry-level: CompTIA Security+, SSCP
    - Intermediate: CISSP, CEH, CySA+
    - Specialized: OSCP (offensive), CISM (management)

Reading & Communities

- Blogs: Krebs on Security, Schneier on Security
- Podcasts: Security Now, Darknet Diaries
- Forums: Reddit r/cybersecurity, Stack Exchange Security

Below is a focused glossary of 50 key cybersecurity terms with concise definitions—ideal for rapid review before an interview. Feel free to print or paste this into your notes.

Term	Definition
Asset	Anything of value (data, hardware, software, personnel) that needs protection.
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organization.
Vulnerability	A weakness in a system, network, or process that can be exploited by a threat actor.
Risk	The potential for loss or damage when a threat exploits a vulnerability. Calculated as: Risk = Likelihood × Impact.
CIA Triad	The foundational model in security—**C**onfidentiality (privacy), **I**ntegrity (accuracy), **A**vailability (uptime).
Exploit	Code or technique that takes advantage of a vulnerability to breach security.
Attack Vector	The path or method by which an attacker gains access (e.g., email, USB, open port).
Malware	Malicious software (virus, worm, Trojan, ransomware, spyware) designed to damage or gain unauthorized access.
Phishing	The use of deceptive emails or sites to trick users into revealing credentials or installing malware.
Social Engineering	Psychological manipulation of people to perform actions or divulge confidential information.
Ransomware	Malware that encrypts files or systems, demanding payment for decryption.
DDoS / DoS	Distributed/Denial-of-Service: Overloading a target's resources to render it unavailable.
Firewall	A network security device or software that filters incoming/outgoing traffic based on rules.
VPN	Virtual Private Network—creates an encrypted tunnel over the internet for secure remote access.
IDS / IPS	Intrusion Detection/Prevention System—monitors network or host activity for malicious behavior and alerts or blocks it.
SIEM	Security Information and Event Management—aggregates logs and alerts for analysis and correlation.
EDR	Endpoint Detection & Response—continuously monitors and responds to threats on endpoints (PCs, servers).
Penetration Testing	Ethical hacking exercises to simulate real-world attacks, find vulnerabilities, and recommend fixes.

Term	Definition
Red Team	A group that mimics adversaries to test an organization's defenses end-to-end.
Blue Team	The defensive team that protects systems and responds to red-team activities or real attacks.
Zero Trust	Security model that assumes no user or device is trusted by default—requires continuous verification.
Zero-Day	A vulnerability unknown to vendors or without a available patch—exploited "on day zero."
Patch Management	The process of acquiring, testing, and installing updates or patches to software and systems.
Hashing	Converting data into a fixed-length string (hash) via an algorithm; used for integrity checks.
Encryption	Transforming data into unreadable form for confidentiality; requires a key to decrypt.
Public Key Infrastructure (PKI)	A framework for managing digital certificates and public-key encryption.
Certificate Authority (CA)	Trusted entity that issues and verifies digital certificates (e.g., SSL/TLS certs).
Multi-Factor Authentication (MFA)	Requiring two or more verification methods (something you know, have, or are).
Single Sign-On (SSO)	A user authentication process that permits one set of credentials to access multiple applications.
Least Privilege	Granting users or systems the minimum access necessary to perform their duties.
Segmentation	Dividing a network into smaller zones to limit an attacker's lateral movement.
Network Address Translation (NAT)	Hides internal IP addresses by mapping them to a single external IP, providing a basic layer of security.
Data Loss Prevention (DLP)	Technologies that detect and prevent unauthorized data exfiltration or leakage.
Backup & Recovery	Processes to create copies of data and restore it if the original is lost or corrupted.
Incident Response (IR)	A structured approach for handling security incidents: preparation, identification, containment, eradication, recovery, lessons learned.
Forensics	The collection, preservation, and analysis of digital evidence following an incident.
Threat Hunting	Proactively searching through networks and systems to detect advanced threats that evade automated defenses.
Security Policy	High-level rules and guidelines that define an organization's security posture and expectations.
Standard Operating Procedure (SOP)	Detailed, step-by-step instructions for routine security tasks and incident handling.

Term	Definition
Business Continuity (BC)	Planning to ensure essential services continue during and after a disruption.
Disaster Recovery (DR)	Strategies and processes to restore systems and data after a catastrophic event.
Compliance	Adherence to laws, regulations, and standards (e.g., GDPR, HIPAA, PCI DSS, ISO 27001).
Cloud Security	Practices and tools to secure cloud infrastructure, platforms, and applications (shared-responsibility model).
Container Security	Securing containerized environments (Docker, Kubernetes)—image scanning, runtime controls.
DevSecOps	Integrating security practices into DevOps workflows—shift-left security testing and automation.
Secure Coding	Writing software with security in mind: input validation, error handling, memory management.
Static Application Security Testing (SAST)	Analyzing source code for vulnerabilities without executing it.
Dynamic Application Security Testing (DAST)	Testing running applications for vulnerabilities (black-box testing).
Bug Bounty	Programs that reward external researchers for reporting security flaws.
Security Orchestration, Automation & Response (SOAR)	Platforms that automate security operations workflows and incident responses.
Security Operations Center (SOC)	A centralized team and facility responsible for monitoring, detecting, and responding to security events.
Key Performance Indicator (KPI)	Metrics used to measure the effectiveness of security controls or processes.
Playbook	Predefined, step-by-step procedures for handling specific types of incidents or tasks.