CS-001 · Foundations

Cybersecurity

Protecting systems, networks, and data from digital attack, loss, and misuse.

Executive Summary

Cybersecurity is the practice of protecting systems, networks, applications, and data from unauthorized access, disruption, theft, and misuse. It combines technology, process, and human behavior to keep information confidential, accurate, and available. It is now a board-level business concern, not just an IT function.

What It Is

Cybersecurity is the discipline of defending digital and connected assets against attackers and accidental harm. It spans everything from the passwords an employee chooses to the architecture of a global cloud platform. The field is commonly organized around the CIA triad: keeping data confidential (only the right people can see it), maintaining its integrity (it is accurate and unaltered), and ensuring its availability (it is there when it is needed). A useful mental model is people, process, and technology working together: the strongest firewall fails if a person is tricked into handing over a password, and the best-trained team fails without tools and clear procedures.

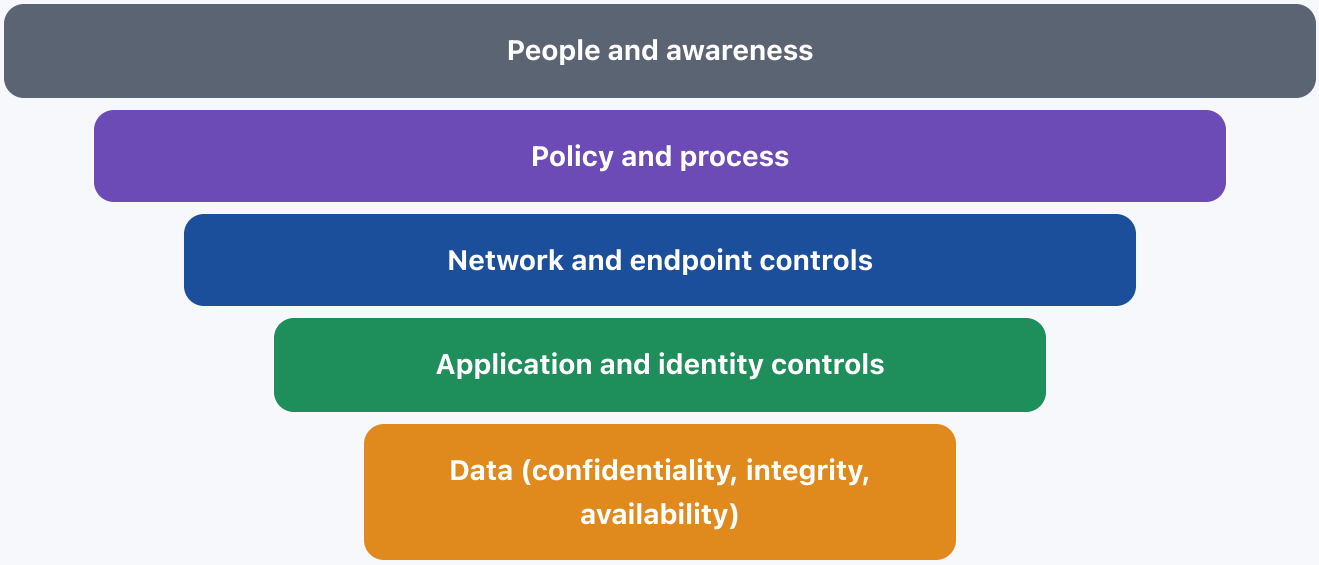
Why It Matters

Nearly every organization now runs on software and data, which means a security failure is a business failure. A single incident can halt operations, expose customer records, trigger regulatory penalties, and erode trust that took years to build. Attackers range from opportunistic criminals to organized ransomware crews and nation-state groups, and the barrier to entry keeps dropping as tools are automated and sold as a service. For professionals, this makes security literacy valuable across almost every role, and it makes dedicated security work one of the most durable career paths in technology.

How It Works

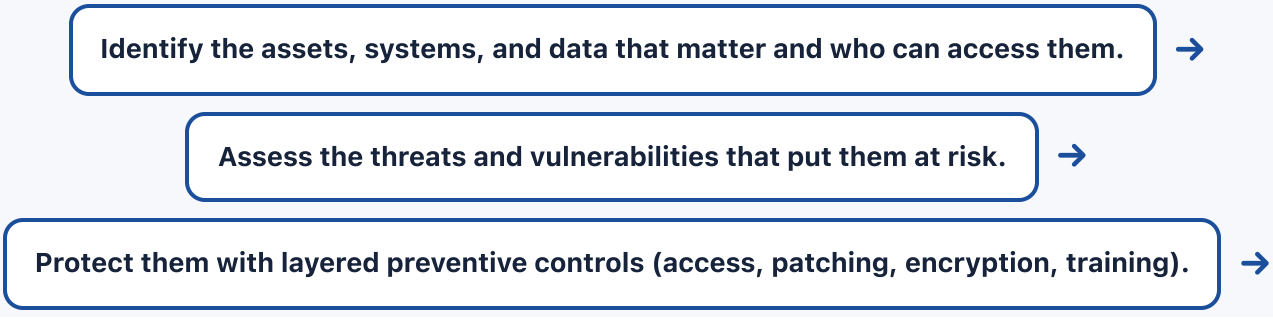
Effective cybersecurity is layered rather than a single product. Organizations identify what they need to protect, assess the risks to it, and apply overlapping controls so that if one fails, others still stand. Preventive controls (such as access management and patching) reduce the chance of a breach; detective controls (such as logging and monitoring) catch what gets through; and responsive controls (such as an incident response plan and backups) limit damage and speed recovery. This maps to the widely used framework of identify, protect, detect, respond, and recover. Security is continuous: threats evolve, systems change, and controls must be tested and improved over time.

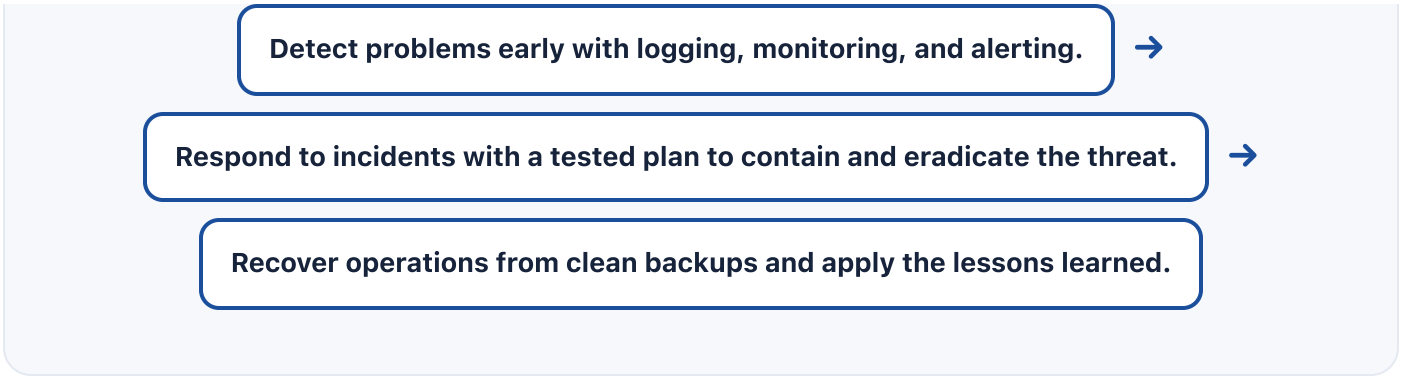
Architecture Diagram



Defense is layered: people and process wrap around technology, which wraps around the data being protected.

Visual Workflow





Common Attacks

- Phishing and social engineering that trick people into granting access
- Ransomware that encrypts data and demands payment
- Credential theft and reuse leading to account takeover
- Exploitation of unpatched software vulnerabilities
- Misconfigured cloud storage and services exposing data

Common Mistakes

- Treating security as a one-time project instead of an ongoing program
- Relying on a single control (for example, a firewall) with no depth behind it
- Leaving known vulnerabilities unpatched because patching is inconvenient
- Giving users far more access than their job requires
- Having backups but never testing that they actually restore

Best Practices

- Adopt a recognized framework (such as the NIST Cybersecurity Framework or CIS Controls) as a baseline
- Enforce multi-factor authentication and least-privilege access
- Patch promptly and maintain an accurate inventory of assets
- Log centrally and monitor for anomalies
- Maintain tested, offline or immutable backups
- Train people continuously and make reporting a suspected incident easy

Quick Checklist

- [x] MFA enabled on all accounts, especially admin and email
- [x] Asset inventory current and owned by someone
- [x] Critical and high vulnerabilities patched on a defined schedule
- [x] Centralized logging in place and reviewed
- [x] Backups tested with a real restore in the last 90 days
- [x] Written, exercised incident response plan

Recommended Tools

Endpoint Detection and Response (EDR)
Monitors endpoints for malicious behavior and enables response

SIEM
Centralizes and correlates logs to surface security events

Vulnerability scanner
Finds known weaknesses across systems and applications

Password manager and MFA app
Strengthens the most-attacked control, credentials

Industry Standards

NIST Cybersecurity Framework (CSF) 2.0
Common language of Govern, Identify, Protect, Detect, Respond, Recover

CIS Critical Security Controls
Prioritized, practical safeguards for getting started

ISO/IEC 27001
International standard for an information security management system

Career Relevance

Cybersecurity underpins roles from SOC analyst, security engineer, and penetration tester to GRC analyst, security architect, and CISO. Even outside dedicated security jobs, fluency in these fundamentals is increasingly expected of developers, IT staff, product managers, auditors, and privacy and AI governance professionals, the audience AI-Governance-Jobs.com serves.

Interview Questions

- What is the CIA triad, and can you give an example of a control for each part?
- Explain defense in depth and why a single control is not enough.
- Walk me through the phases of the NIST incident response lifecycle.
- How would you prioritize which vulnerabilities to fix first?
- Why is multi-factor authentication so effective against common attacks?

Related Certifications

CompTIA Security+ **ISC2 Certified in Cybersecurity (CC)** **ISACA CISM (for leadership tracks)**

Further Reading

- NIST Cybersecurity Framework 2.0
- CISA: Cybersecurity Best Practices
- CIS Critical Security Controls

Key Takeaways

- Cybersecurity protects the confidentiality, integrity, and availability of systems and data.
- It is people, process, and technology together, not any single tool.
- Strong programs are layered: prevent, detect, and respond.
- It is a continuous program tied directly to business risk.

- Fundamentals here are career-relevant across security, IT, GRC, privacy, and AI governance.

FAQ

Is cybersecurity the same as information security?

Do I need to code to work in cybersecurity?

Where should a beginner start?

Related Careers

RELATED ROLES

Soc Analyst | Grc Analyst | Security Engineer

RELATED CERTIFICATIONS

CompTIA Security+ | ISC2 Certified in Cybersecurity (CC) | ISACA CISM (for leadership tracks)

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Study this sheet: **Cybersecurity**
2. Go deeper: The CIA Triad
3. Go deeper: Defense in Depth
4. Validate it: work toward **CompTIA Security+**

5. Find the role: browse current openings

RELATED SHEETS

CS-002 The CIA Triad | CS-003 Defense in Depth | CS-004 Zero Trust | CS-009 Core Security Principles | CS-010 Cyber Hygiene