Cybersecurity Fundamentals

Introduction to Information Security

What is Information Security?

- Protection of information from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Ensures confidentiality, integrity, and availability (CIA Triad).
- Example: Protecting login credentials from being shared or stolen.

Why is Information Security Important?

- Safeguards sensitive data (e.g., personal, financial, and health information).
- Prevents identity theft and fraud.
- Protects business assets and reputation.
- Ensures compliance with laws and regulations (e.g., GDPR, HIPAA).
- Example: A healthcare provider encrypting patient records to comply with HIPAA regulations.

Information Security v/s Cyber Security

Hack

Cutting something into pieces by sheer force

Doing anything in an unconventional way or in a shortcut way

Hacker and Types of Hacker

- Black hat
- White hat
- Gray hat
- Script kiddies
- Suicidal hackers
- State-sponsored hackers
- Cyberterrorists
- Hacktivists
- Insider Threats
- Advanced Persistent Threat (APT)

Common Threats

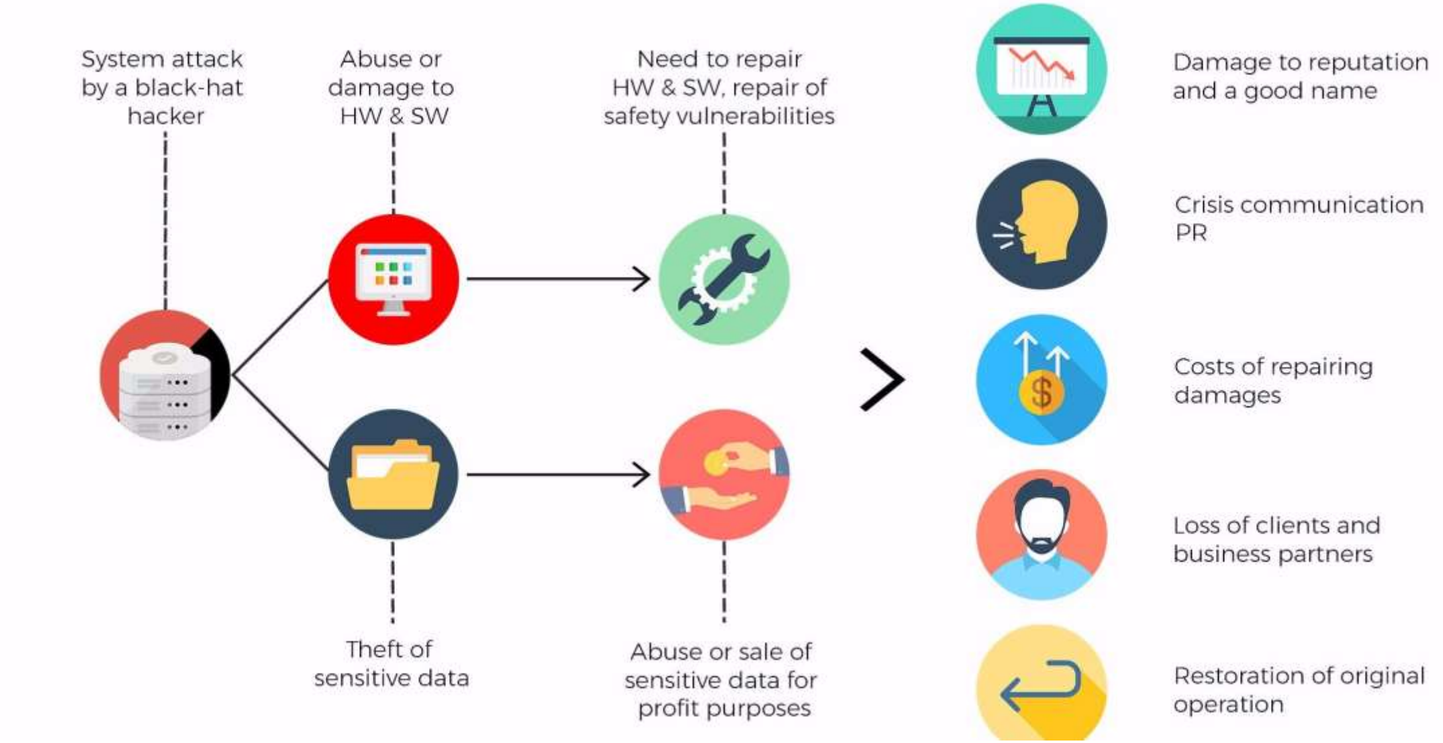
- Malware: Viruses, worms, and ransomware.
- Phishing: Deceptive emails to steal sensitive information.
- Physical Theft: Devices being stolen or misplaced.
- Social Engineering: Manipulating individuals to divulge confidential information.
- Denial-of-Service (DoS) Attacks: Overloading systems to make services unavailable.
- Man-in-the-Middle (MitM) Attacks: Intercepting communication between two parties.
- SQL Injection: Exploiting vulnerabilities in databases to steal or manipulate data.
- Zero-Day Vulnerabilities: Exploiting unknown software vulnerabilities.
- Data Breaches: Unauthorized access to sensitive data.
- IoT Vulnerabilities: Exploiting weak security in Internet of Things devices.
- Unpatched Software: Exploiting known vulnerabilities in outdated software.
- Rogue Access Points: Unauthorized wireless access points allowing network intrusion

Basic Security Terminologies

- Vulnerability
- Exploit
- Attack
- Payload
- Asset
- Asset value
- Hack value
- Risk
- Threat
- Bot
- Bot-net
- Trojan
- Daisy chaining
- Personally identifiable information
- Doxing

Impacts of Hack

- Reputational impact
- Operational impact
- Financial impact
- Legal impact



Elements of Information Security

Confidentiality

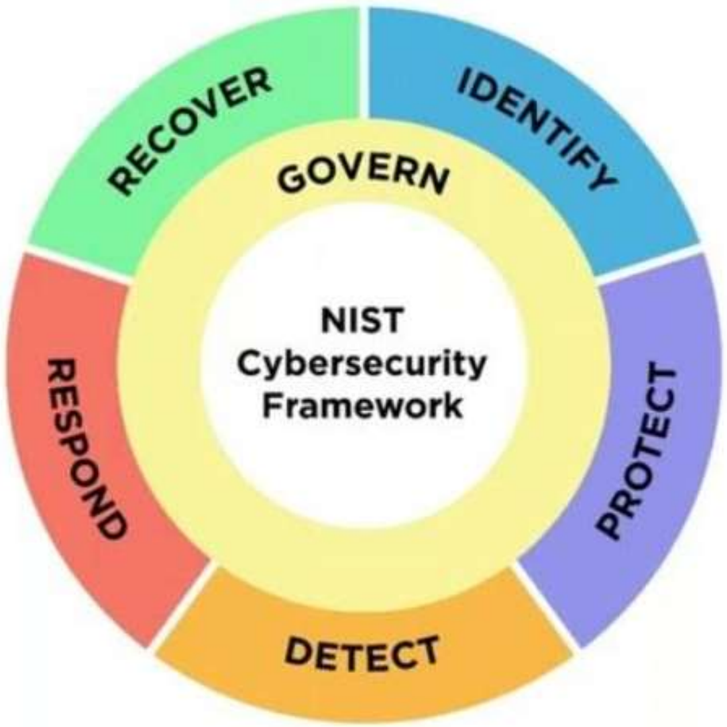
Integrity

Availability

Authenticity

Non-Repudiation

NIST Cyber Security Framework



Function	Purpose
Identify	Help determine the current cybersecurity risk to the organization
Protect	Use safeguards to prevent or reduce cybersecurity risk
Detect	Find and analyze possible cybersecurity attacks and compromises
Respond	Take action regarding a detected cybersecurity incident
Recover	Restore assets and operations that were impacted by a cybersecurity incident
Govern (new!)	Establish and monitor the organization's cybersecurity risk management strategy, expectations & policy

ISO/IEC 27001 Framework

CIS Critical Security Controls (CIS CSC)

Identity and Access Management (IAM)

Identity and Access Management (IAM)

- **Identity and Access Management (IAM)** is a security framework that ensures **the right person gets the right access to the right resource at the right time.**
  - **Identity** = Who are you? (user, employee, admin, app, service)
  - **Access** = What are you allowed to do? (read, write, delete, approve)
- IAM is used in **organizations, cloud platforms, applications, networks, and databases** to control user access securely.

Core Components of IAM

- Identity: A user or system that needs access.
- Authentication: Verifying the identity of users.
- Authorization: Granting access to resources.
- IGA – Identity Governance & Administration: ensures that access is appropriate, approved, and regularly reviewed for compliance
- SoD – Segregation of Duties: Ensures that critical or conflicting tasks are divided among multiple users
- CIAM – Customer Identity & Access Management: Manages identities and access for external users such as customers and partners
- Privileged Access Management (PAM): Secures and monitors high-privilege accounts such as administrators and root users
- Single Sign-On (SSO): Allows users to authenticate once and gain access to multiple applications
- Accounting (Audit, Logging, and Monitoring): Tracking and recording user activities.

Authentication

- The process of verifying who you are.
- Methods:
  - Something you know: Passwords, PINs.
  - Something you have: Smart cards, tokens.
  - Something you are: Biometrics (fingerprint, facial recognition).

  Example: Logging into a bank account using a password and OTP.

Authorization

- Determining what actions a user is allowed to perform.
- Key Concepts:
  - Role-based access control (RBAC).
  - Least privilege principle.
  - Access control lists (ACLs).

  Example: A marketing employee accessing customer data but not financial records.

Accounting

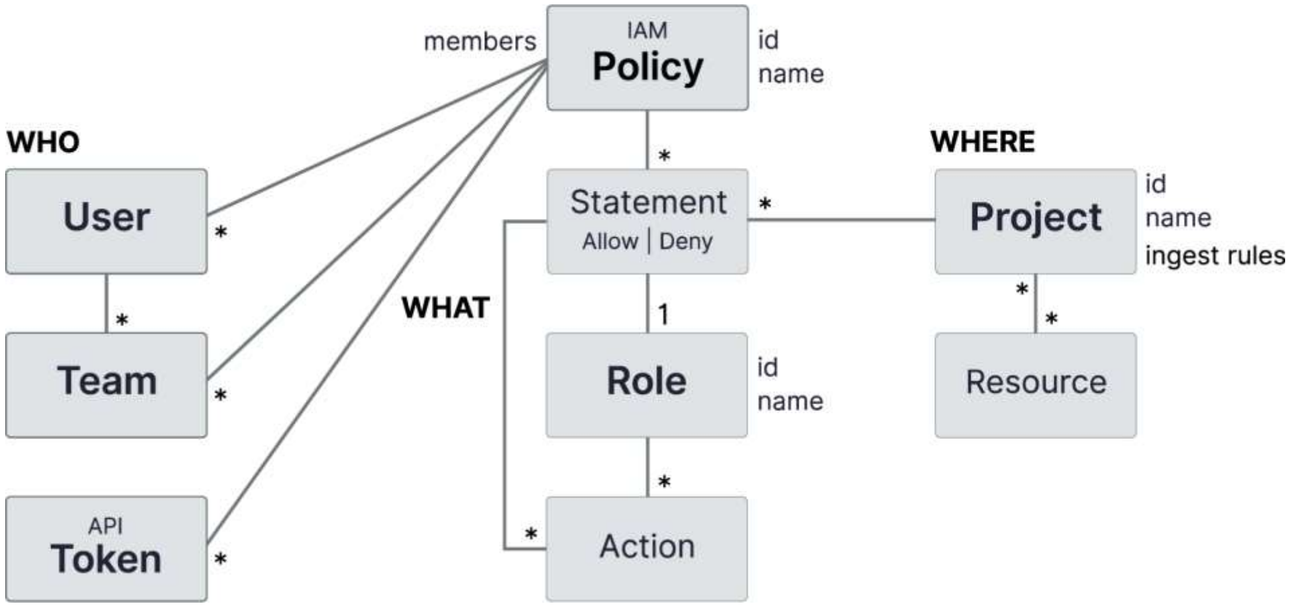
- Tracking and logging user activities.
- Purpose:
  - Monitoring resource usage.
  - Auditing for security and compliance.
  - Detecting anomalies and incidents.

  Example: Logging IP addresses and timestamps for VPN sessions.

IAM Policies

- An **IAM policy** is a **set of rules** that defines:
  - **Who** can access a resource
  - **What actions** they can perform
  - **On which resources**

- Core Components of an IAM Policy
  - **1. Subject (Who)**
  - **2. Action (What)**
  - **3. Resource (On What)**
  - **4. Effect (Allow or Deny)**
  - **5. Condition (When / How)**



Types of IAM Policies

1. Identity-Based Policies
2. Resource-Based Policies
3. Role-Based Access Control (RBAC) Policies
4. Attribute-Based Access Control (ABAC)
5. Privileged Access Policies

IAM Implementation Strategies

1. Zero-Trust Policy
2. Secure Access
3. Secured Privileged Accounts
4. Central Identity Management
5. Policy Based Control
6. Training and Support

IAM Lifecycle (Identity and Access Management)

IAM lifecycle defines how a user's digital identity and access rights are created, managed, monitored, and removed across systems during their association with an organization.

1. Identity Creation
2. Provisioning (Access Assignment)
3. Authentication (Identity Verification)
4. Authorization (Access Enforcement)
5. Access Review & Monitoring (Governance Phase)
6. Privileged Access Management (PAM)
7. Identity Modification (Mover Phase)
8. De-Provisioning (Leaver Phase)
9. Audit, Compliance & Reporting


thank you