

Chapter 1 – Foundations of Cyber Security

Introduction

We live in a digital world. Almost everything today uses computers and the Internet.

Examples include: Mobile Banking, UPI Payments, Social Media, Online Shopping, Government Services, Hospitals, Schools and Colleges, Railway Reservation, Electricity Billing

All these systems store important information such as: Name, Address, Aadhaar Number, PAN Card, Bank Details, Passwords, Medical Records, Business Data

If someone steals or changes this information, it can cause serious problems.

Cyber Security helps protect this information.

What is Cyber Security?

Cyber Security is the practice of protecting computers, mobile phones, networks, software, and data from cyber-attacks, unauthorized access, damage, or theft.

In simple words: Cyber Security means protecting digital information from bad people called cyber criminals.

A computer system needs protection. Computers use: Passwords, Firewalls, Antivirus, Encryption and Multi-Factor Authentication (MFA).

Why is Cyber Security Needed?

Today almost everyone uses the Internet. If these systems are attacked,

- Money can be stolen. Data can be deleted. Personal information can leak. Services may stop working.

Therefore, cyber security is necessary.

Goals of Cyber Security

Cyber Security has many goals.

Goal 1 Protect Data. Example: Protect student marks from hackers.

Goal 2 Protect Privacy. Example: Only doctors should see patient records.

Goal 3 Protect Money. Example: Prevent online banking fraud.

Goal 4 Protect Systems. Example: Prevent viruses from damaging computers.

Goal 5 Provide Safe Communication. Example: Secure online shopping using HTTPS.

What Does Cyber Security Protect?

Cyber Security protects: Computers, Mobile Phones, Servers, Websites, Databases, Networks, Cloud Systems, IoT Devices, Smart TVs, Smart Watches, and CCTV Cameras

Example Table

Asset	Why Protect?
Laptop	Personal files
Mobile Phone	Banking Apps
Website	Customer Services
Database	Student Records
Network	Company Communication
Cloud Storage	Company Data

Common Cyber Threats

A cyber threat is something that can harm a computer system.

Common threats include:

Virus: A virus damages files and spreads to other computers.

Example: An infected pen drive spreads a virus.

Worm: A worm spreads automatically through a network. It does not need user action.

Trojan Horse: Looks like useful software. Actually contains malware.

Example: Fake game downloaded from an unknown website.

Ransomware: Locks your files. The attacker demands money.

Example: Your photos become inaccessible until a ransom is paid.

Phishing: Fake emails or websites steal information.

Example: Fake bank email asking for your password.

Spyware: Secretly monitors your activities.

Example: Records passwords.

Keylogger: Records every key you press.

Example

Typing password



Keylogger saves it



Hacker steals it

Who Needs Cyber Security? Everyone.

Students: Protect assignments and emails.

Teachers: Protect examination papers.

Banks: Protect money.

Hospitals: Protect patient records.

Government: Protect national data.

Companies: Protect business information.

Individuals: Protect photos, passwords, and documents.

Cyber Crime

Cyber-crime is a crime committed using computers or the Internet.

Examples: Hacking, Identity Theft, Online Fraud, Credit Card Fraud, ATM Fraud, Cyber Bullying, Fake Websites, and Data Theft.

Example

A hacker steals someone's ATM password. Withdraws ₹50,000. This is cyber-crime.

Cyber Attack

A cyber-attack is an attempt to damage, steal, or destroy digital information.

Examples: Virus attack, DDoS attack, Ransomware attack, SQL Injection, Password attack, and Phishing attack

Difference Between Cyber Security and Cyber Crime

Cyber Security	Cyber Crime
Protection	Crime
Prevents attacks	Performs attacks
Legal activity	Illegal activity
Uses security tools	Uses hacking tools

Benefits of Cyber Security

- Protects personal information.
- Prevents hacking.
- Secures online banking.
- Protects businesses.
- Prevents financial loss.
- Increases customer trust.
- Protects government information.
- Ensures continuous business operations.

Everyday Examples

Example 1: Using fingerprint unlock on your phone. This is cyber security.

Example 2: Receiving OTP while logging into banking. This is Multi-Factor Authentication (MFA).

Example 3: Using antivirus software. This is endpoint protection.

Example 4: Shopping only on websites that use HTTPS. This protects your payment information.

- **Cyber Security protects computers, networks, software, and digital data.**
- It helps keep information confidential, accurate, and available.
- **Cyber threats include viruses, ransomware, phishing, spyware, and keyloggers.**
- Cyber Security is important for individuals, businesses, governments, hospitals, schools, and banks.

- **Good security habits, such as using strong passwords and checking for HTTPS, reduce the risk of cyber attacks.**

Important Keywords

Term	Meaning
Cyber Security	Protection of digital systems
Cyber Attack	Attempt to damage systems
Cyber Crime	Crime using computers
Malware	Harmful software
Virus	Program that infects files
Ransomware	Locks files and demands money
Phishing	Fake messages to steal information
Firewall	Filters network traffic
Antivirus	Detects and removes malware

Exercise 1 – Check Website Security

Objective

Learn to identify a secure website.

Requirements

- . Internet connection
- . Web browser

Steps

- 1.Open your browser.
- 2.Visit a trusted website, such as your bank or a major shopping site.
- 3.Check if the address starts with **https://**.
- 4.Look for the padlock icon in the address bar.
- 5.Click the padlock to view certificate information (do not change any settings).

Observation

- Websites using **HTTPS** encrypt data between your browser and the server.
- The padlock indicates a secure connection, but you should still verify that the website address is correct.

Result

You successfully identified whether a website uses a secure connection.

Exercise 2 – Create a Strong Password

Objective

Create a password that is difficult to guess.

Weak Password

rahul123

Strong Password Example

R@hul#2026!Study

Rules for a Strong Password

- At least 12 characters long
- Use uppercase and lowercase letters
- Include numbers
- Include special symbols
- Avoid using your name, birthday, or simple words

Result

You created a stronger password following recommended security practices.

Need of Cyber Security

Today, computers and the Internet are used almost everywhere.

We use them for: Online Banking, Mobile Payments (UPI), Shopping, Education, Hospitals, Government Services, Entertainment, Social Media, Business

Since almost everything is digital, a large amount of important information is stored online.

This information includes: Personal information, Bank details, Passwords, Medical records, Business secrets, Government records, If this information falls into the wrong hands, it can cause serious damage.

Therefore, cyber security has become a basic necessity.

Why Do We Need Cyber Security?

Cyber security protects people, businesses, and governments from cyber attacks.

Without cyber security: Computers may stop working, Data may be stolen, Money may be lost, Privacy may be violated, Business operations may stop.

Example

Imagine you have ₹20,000 in your bank account. A hacker steals your banking password. The hacker transfers all your money to another account. Without proper cyber security, recovering the money may take a long time and may not always be possible.

Importance of Cyber Security in Daily Life

Almost everyone uses digital devices.

Students: Students use: Online classes, Email, College portals, Cloud storage.

Cyber security helps protect: Assignments, Personal information, Exam records

Teachers: Teachers use: Student databases, Examination systems, Research papers.

Cyber security prevents unauthorized access to these records.

Hospitals: Hospitals store: Patient records, Medical history, Test reports, X-rays, Prescriptions.

If these records are stolen or changed, patient care can be affected.

Banks: Banks store: Account numbers, ATM PINs, Transaction history, Credit card details.

Cyber security protects customers from online fraud.

Government Governments store: Aadhaar information, Passport records, Tax information, Election data.

Cyber security protects national information from attackers.

Businesses: Businesses store: Customer information, Employee records, Financial reports, Product designs, and Business plans.

Cyber security helps prevent data theft and financial loss.

What Can Happen Without Cyber Security?

Without cyber security, many problems can occur.

Data Theft: Attackers steal confidential information.

Example: A hacker steals customer details from an online shopping website.

The stolen information is sold illegally.

Financial Loss: Cyber criminals steal money.

Example: A fake banking website asks users to enter their username and password.

The attacker then transfers money from the victim's account.

Identity Theft: Someone pretends to be another person.

Example: A hacker uses another person's Aadhaar number to apply for loans or create fake accounts.

Loss of Privacy: Private information becomes public.

Example: Personal photos stored in cloud storage are leaked online.

Business Loss: Businesses may lose customers and reputation.

Example: If a company's website is hacked and customer information is stolen, customers may stop using its services.

Service Disruption: Some attacks stop important services.

Example: A hospital's computer system is infected with ransomware, making patient records temporarily unavailable.

Areas Where Cyber Security Is Needed

Cyber security is important in many sectors.

Sector	Why Cyber Security Is Needed	
Banking	Protect money and customer accounts	
Education	Protect student information	
Healthcare	Protect medical records	
Government	Protect national data	
Defence	Protect military information	
E-commerce	Secure online shopping	
Transportation	Protect railway and airline systems	
Telecommunications	Secure communication networks	

Modern Technologies That Need Cyber Security

Technology has made life easier, but it also creates new security challenges.

Cloud Computing: People store files on cloud services.

Examples: Google Drive, Microsoft OneDrive, Dropbox.

Cyber security protects cloud data from unauthorized access.

Internet of Things (IoT): IoT devices include: Smart TVs, Smart Watches, Smart Cameras, Smart Refrigerators, Smart Speakers

If not secured, attackers may control these devices.

Mobile Phones: Smartphones store: Photos, Banking apps, Contacts, Emails

A lost or infected phone can expose personal information.

Social Media: Examples: Facebook, Instagram, X (formerly Twitter), LinkedIn

Users should avoid sharing sensitive personal information and use strong passwords with two-factor authentication.

Common Reasons for Cyber Attacks

Cyber criminals attack systems for different reasons.

Money: They steal money from individuals or businesses.

Personal Information: Personal data can be sold illegally or misused.

Business Secrets: Competitors or criminals may try to steal valuable business information.

Political Reasons: Some attacks target governments or public institutions.

Entertainment or Curiosity: Some inexperienced attackers may try to break into systems without fully understanding the consequences.

Impact of Cyber Attacks

Cyber attacks affect many people.

On Individuals: Loss of money, Identity theft, Privacy violations, Stress and inconvenience

On Businesses: Financial losses, Loss of customer trust, Legal issues, Operational downtime

On Government: Disruption of public services, Data breaches, Risks to national security

On Society: Reduced trust in digital systems, Economic losses, Disruption of essential services

Benefits of Cyber Security

Good cyber security helps to: Protect confidential information, reduce cyber-attacks, Protect bank accounts, Secure online payments, Prevent identity theft, Protect business data, Keep services running, Increase trust in digital systems.

Everyday Examples

Example 1 – Online Shopping

You buy a mobile phone from a trusted shopping website. The website uses HTTPS and encrypts your payment details. Your information is protected during the transaction.

Example 2 – UPI Payment

You receive an OTP before completing a transaction. Even if someone knows your password, they cannot complete the payment without the OTP.

Example 3 – School Portal

A student logs into the college portal. Only the student can view their own marks after successful authentication.

Example 4 – Hospital

Doctors access patient records using secure login credentials. Unauthorized users cannot view or modify patient information.

Exercise 1 – Enable Two-Factor Authentication (2FA)

Objective

Learn how to improve account security.

Requirements

- A Google, Microsoft, or other online account that supports 2FA

Steps

1. Log in to your account.
2. Open **Security Settings**.
3. Find **Two-Step Verification** or **Two-Factor Authentication**.
4. Enable it.
5. Follow the setup instructions using an authenticator app or SMS (if available).

Observation

You are now asked for a second verification step during login.

Result: Your account is more secure because a password alone is no longer enough to log in.

Exercise 2 – Identify a Phishing Email

Objective

Learn to recognize suspicious emails.

Steps

Look for these warning signs:

- . Unknown sender
- . Urgent requests (e.g., "Your account will be closed today!")
- . Spelling or grammar mistakes
- . Suspicious links
- . Requests for passwords or OTPs

Observation

Legitimate organizations generally do **not** ask for passwords or OTPs by email.

Result: You can better identify phishing attempts.

Summary

- Cyber security is essential because modern life depends on digital systems.
- It protects people, businesses, and governments from cyber threats.
- Strong security practices reduce financial losses, protect privacy, and maintain trust.
- Simple measures like strong passwords, HTTPS, and 2FA significantly improve security.

Key Terms

Term	Meaning
Cyber Security	Protection of digital systems and data
Data Theft	Stealing confidential information
Identity Theft	Using another person's identity illegally
Phishing	Fake messages designed to steal information
Two-Factor Authentication (2FA)	Login method requiring two forms of verification
Encryption	Converting data into a secure format to prevent unauthorized access

Information Security vs Cyber Security

They are closely related, but **they are not exactly the same.**

- **Information Security** protects **all information**, whether it is on paper, in a computer, or spoken.
- **Cyber Security** mainly protects **digital systems** connected to computers and networks.

Simple Example

Imagine a college. The college has:

- Student records on paper
- Student records stored in a computer
- CCTV system
- College website

Information Security protects **all of these records**, including paper files.

Cyber Security mainly protects the **computer systems, website, network, and digital records.**

What is Information Security?

Information Security (InfoSec) is the practice of protecting information from unauthorized access, use, disclosure, modification, destruction, or loss.

It protects information in **any form.**

Information can be: Paper documents, Computer files, Mobile phone data, Emails, Cloud storage, USB drives, Printed reports, Spoken confidential information.

Simple Definition: Information Security means **keeping information safe no matter where it is stored.**

Goals of Information Security

Information Security aims to:

- Keep information confidential
- Prevent unauthorized changes
- Ensure information is available when needed
- Protect against theft
- Protect against accidental loss

What is Cyber Security?

Cyber Security is the practice of protecting digital devices, networks, applications, and data from cyber attacks.

It mainly focuses on digital systems.

Cyber Security protects: Computers, Mobile phones, Servers, Networks, Websites, Applications, Cloud systems, Databases, IoT devices.

Cyber Security means protecting digital technology from cyber attacks.

Example

A company's website is attacked by hackers. Cyber Security tools such as: Firewall, Antivirus, Intrusion Detection System (IDS), Encryption, Multi-Factor Authentication (MFA), help protect the website.

Information Security vs Cyber Security

Information Security	Cyber Security
Protects all types of information	Protects digital systems and data
Covers paper & digital records	Focuses mainly on digital information
Includes physical security	Includes network & computer security
Wider concept	Part of Information Security
Protects CIA of information	Protects against cyber-attacks and online threats

Similarities

Both aim to: Protect valuable information, Prevent unauthorized access, Maintain confidentiality, Ensure integrity, Ensure availability, Reduce risks, Support business operations

Key Differences

Information Security Protects **all information**.

Includes: Paper, Digital, Verbal information.

Cyber Security Protects **digital assets** only.

Includes: Networks, Computers, Mobile phones, Servers, Websites

Information Security protects against: Theft of paper documents, Information leakage, Unauthorized disclosure, Physical damage (fire, flood)

Cyber Security protects against: Malware, Hacking, Phishing, Ransomware, Denial-of-Service (DoS) attacks

Security Methods

Information Security Locked cabinets, Visitor registers, Security guards, Access policies, Data classification, Employee awareness.

Cyber Security Firewalls, Antivirus, Encryption, MFA, Security monitoring, Network segmentation.

Why Both Are Important

Organizations need both Information Security and Cyber Security.

For example:

A company protects:

- Printed contracts

- . Employee records
- . Company laptops
- . Cloud storage
- . Business emails

If only Cyber Security is used, paper documents may still be stolen.

If only Information Security is used, hackers may still attack digital systems.

A complete security program includes both.

Cyber Security is a part of Information Security.

Summary

- **Information Security** protects all information, whether physical, digital, or verbal.
- **Cyber Security** focuses on protecting digital systems, networks, and online data.
- Cyber Security is **one part of the broader field of Information Security**.
- Both are essential because organizations manage information in multiple forms.
- Understanding the distinction helps in choosing the right security controls for different situations.

Key Terms

Term	Meaning
Information Security (InfoSec)	Protects information in any form
Cyber Security	Protects digital systems and networks
Cyber Security	Protects digital systems and networks
Confidentiality	Prevents unauthorized disclosure of information
Integrity	Ensures information remains accurate and unaltered

Exercise 1 – Identify Information Assets

Objective

Learn to classify information assets.

Task

Look around your classroom or home and identify examples of:

Information Asset	Type
Student ID card	Physical
Assignment PDF	Digital
College Notice	Paper
Email	Digital
Notebook	Physical
Pen Drive	Digital
Printed Certificate	Physical

Observation

Information exists in many forms, and each type needs appropriate protection.

Result

You identified different types of information assets.

Exercise 2 – Compare Security Measures

Objective

Understand the difference between Information Security and Cyber Security controls.

Situation	Information Security	Cyber Security
Student records	Locked cabinet	Password-protected database

Office documents	Restricted office access	File encryption
Customer database	Access policy	Firewall and MFA
Employee records	Secure archive	Secure HR application

Result

You learned that different types of information require different protection methods.

Privacy vs Security

They are related, but they are **different concepts**.

Think about your **house**:

- . You lock your door to keep thieves out. This is **Security**.
- . You close your curtains so strangers cannot see inside. This is **Privacy**.

In the digital world:

- . **Security** protects your data from attacks.
- . **Privacy** controls **who is allowed to see or use your personal information**.

Both are necessary.

What is Privacy?

Privacy is the right of a person to control how their personal information is collected, used, shared, and stored.

Simple Definition: Privacy means **keeping your personal information under your control.**

Only the people or organizations you allow should be able to use your information.

Example

Suppose you register on a shopping website.

The website asks for: Name, Phone number, Address, Email etc....

If the website sells your information to another company without your permission, your **privacy is violated.**

Why is Privacy Important?

Privacy protects people from: Identity theft, Financial fraud, Stalking, Spam messages, Unwanted advertisements, Misuse of personal information, Reputation damage.

Example: You upload private family photos to cloud storage. Only you and your family should be able to access them. If strangers can see them without your permission, your privacy has been compromised.

What is Security?

Security means protecting information, systems, and devices from unauthorized access, attacks, damage, or theft.

Simple Definition: Security means **keeping information and systems safe.**

Examples: Security protects: Computers, Mobile phones, Networks, Websites, Databases, Cloud storage, Applications.

Example

A bank uses: Firewalls, Encryption, Antivirus software, Multi-Factor Authentication (MFA), These measures improve the security of customer accounts.

Difference Between Privacy and Security

Privacy	Security
Controls who can access personal information	Protects systems and data from attacks
Focuses on personal rights	Focuses on protection mechanisms
Concerned with data collection and sharing	Concerned with preventing unauthorized access
Personal information is the main focus	Information systems are the main focus
Answers "Who can use my data?"	Answers "How do we protect the data?"

Easy Example

Imagine a hospital.

Privacy: Only the patient and authorized doctors should see the medical report.

Security: The hospital protects the computer system using passwords and encryption.

Another Example

Imagine your mobile phone.

Privacy means: Only you decide who can see your photos and contacts.

Security means: Your phone is protected with a PIN, fingerprint, or face recognition.

Relationship Between Privacy and Security

Privacy and Security work together.

Without Security: Hackers may steal personal information.

Without Privacy: Organizations may misuse personal information even if it is technically secure.

Threats to Privacy: Some common privacy threats include:

Data Collection Without Permission: A website collects more personal information than necessary.

Data Sharing: A company shares your personal information without your consent.

Location Tracking: Some apps collect your location continuously.

Social Media Oversharing: Posting personal details publicly can increase privacy risks.

Identity Theft: A criminal uses someone else's personal information for fraud.

Threats to Security

Some common security threats include: Malware, Viruses, Worms, Trojan horses, Ransomware, Phishing, Password attacks, Denial-of-Service (DoS) attacks, Insider threats

How to Protect Privacy?

Follow these good practices: Share only necessary personal information. Read privacy settings before using apps. Limit who can view your social media profile. Avoid posting sensitive information online. Be cautious when granting app permissions (such as access to your camera, microphone, or location). Use trusted websites and applications.

How to Improve Security

Some simple security measures include: Use strong passwords. Enable Multi-Factor Authentication (MFA). Keep software updated. Install reputable antivirus software. Avoid downloading software from untrusted sources. Use HTTPS websites. Lock your devices with a PIN, password, or biometric authentication. Back up important data regularly.

Remember these points:

- **Privacy** gives people control over how their personal information is collected, used, and shared. **Security** protects systems and data from unauthorized access, attacks, and damage. Privacy and Security are different but closely connected.
- Strong security measures help protect privacy, while privacy policies guide the responsible use of personal information. Following good digital habits, such as reviewing app permissions, using strong passwords, and enabling MFA, helps protect both privacy and security.
- **Privacy** is about **control over personal information**.
- **Security** is about **protecting information and systems**.
- Good security supports privacy, but security alone does not guarantee privacy.

- Organizations should implement both privacy practices and security controls.

- **Key Differences (Quick Revision)**

Privacy	Security
Protects personal information	Protects systems and data
Controls who may access information	Prevents unauthorized access
Focuses on user rights and consent	
Concerned with proper use of data	Concerned with defending against attacks

Exercise 1 – Review App Permissions

Objective

Understand how apps access personal information.

Requirements

An Android or iPhone device.

Steps

1. Open **Settings**.
2. Go to **Privacy** or **Privacy & Security**.
3. Open **Permissions**.
4. Review apps that can access:
 - Camera
 - Microphone
 - Location

- Contacts
- Photos

5. Disable permissions that are not necessary.

Observation

Many apps request permissions that are not essential for their core function.

Result

You improved your privacy by limiting unnecessary access.

Exercise 2 – Check Privacy Settings on a Social Media Account

Objective

Learn how to control who can see your information.

Steps

1. Open your social media account.
2. Go to **Privacy Settings**.
3. Review:
 - Who can see your profile?
 - Who can send you friend requests?
 - Who can see your posts?
4. Adjust the settings to match your preferences.

Result

You increased the privacy of your online profile.

Exercise 3 – Security Check

Objective

Review the security of an online account.

Steps

1.Open your account's **Security Settings**.

2.Check whether:

- A strong password is being used.
- Multi-Factor Authentication (MFA) is enabled.
- Recovery email and phone number are correct.

3.Update any outdated information.

Result

You improved the security of your account.

Governance

Imagine a school without any rules?

Students can enter any classroom?

Teachers can change marks without permission?

Anyone can enter the principal's office?

No attendance records are maintained?

Would the school work properly?

No.

Every organization needs **rules, responsibilities, and proper management.**

Similarly, organizations also need rules for protecting their digital systems and information. These rules are called **Cyber Security Governance.**

What is Governance?

Governance is the process of directing, controlling, and managing an organization to achieve its goals while following laws, policies, and ethical practices.

Simple Definition: Governance means making rules, assigning responsibilities, and ensuring everyone follows them.

Example

In a college:

Principal → Makes important decisions.

Teachers → Follow college rules.

Students → Follow classroom rules.

Administration → Maintains records.

Everyone has different responsibilities.

The same idea applies to cyber security.

What is Cyber Security Governance?

Definition: Cyber Security Governance is the system of rules, policies, responsibilities, and processes that helps an organization protect its information and technology. It ensures that cyber security supports the organization's goals and is managed effectively.

Simple Definition: Cyber Security Governance means **planning, managing, and monitoring security so that everyone knows what to do.**

Example A company decides that:

- . Every employee must use a strong password.
- . Passwords must be changed regularly.
- . Only authorized employees can access company data.
- . All computers must have antivirus software.
- . Security training is conducted every year.

These are examples of cyber security governance.

Why is Governance Important?

Without governance:

- Employees may not know security rules.
- Sensitive data may be exposed.
- Different departments may follow different practices.
- Security incidents may increase.
- The organization may violate laws or regulations.

Benefits of Governance

Good governance helps an organization: Protect important information. Reduce cyber risks. Improve customer trust. Meet legal and regulatory requirements. Clearly define responsibilities. Respond effectively to security incidents. Support business continuity.

Objectives of Cyber Security Governance

The main objectives are:

- 1. Protect Information:** Keep data safe from unauthorized access.
- 2. Manage Risks:** Identify and reduce cyber risks before they cause harm.
- 3. Support Business Goals:** Security should help the organization operate safely and efficiently.
- 4. Ensure Compliance:** Follow applicable laws, regulations, and organizational policies.
- 5. Improve Decision-Making:** Provide management with information to make informed security decisions.

Key Components of Cyber Security Governance

A good governance program includes: Policies, Standards, Procedures, Guidelines, Risk Management, Compliance, Audits, Training and Awareness, Incident Response.

Security Policies

Definition: A **Security Policy** is a high-level document that explains an organization's security rules and expectations.

Simple Definition: A policy tells employees **what must be done**.

Examples

- Use strong passwords. Do not share passwords. Lock your computer when leaving your desk. Report suspicious emails. Install only approved software.

Example: A college policy may state: Students must not share their login passwords with anyone.

Standards

Definition: Standards provide specific and mandatory technical requirements to support policies.

Simple Definition: Standards explain **how something should be done consistently**.

Example: Password Standard.

Procedures

Definition: Procedures describe the exact steps to perform a task.

Simple Definition: A procedure explains **how to do a task step by step**.

Example: Password Reset Procedure.

Guidelines: Guidelines are recommended best practices. They are advisory rather than mandatory.

Simple Definition: Guidelines suggest the best way to perform a task.

Difference Between Policy, Standard, Procedure, and Guideline

Item	Purpose	Mandatory?	Example
Policy	States what must be done	Yes	Use strong passwords
Standard	Defines specific requirements	Yes	Password must be at least 12 characters
Procedure	Explains step-by-step actions	Yes	Steps to reset a password
Guideline	Recommends best practices	Usually No	Use a password manager

Roles and Responsibilities

Cyber security is everyone's responsibility.

Different people have different roles.

Senior Management

Responsibilities: Approve security policies. Allocate budget. Support security initiatives.

IT Department

Responsibilities: Manage servers. Configure networks. Install security updates. Monitor systems.

Security Team

Responsibilities: Monitor threats. Investigate incidents. Conduct risk assessments. Perform security testing.

Employees

Responsibilities: Follow security policies. Use strong passwords. Report suspicious activity. Complete security awareness training.

Risk Management

Definition: Risk Management is the process of identifying, assessing, and reducing risks.

Four Basic Steps

1. Identify risks.
2. Analyze the risks.
3. Reduce or treat the risks.
4. Monitor the risks.

Compliance

Definition: Compliance means following applicable laws, regulations, and organizational policies.

Simple Definition: Compliance means following the required rules.

Examples

A company may need to comply with: Data protection laws, Banking regulations, Healthcare regulations, Internal company policies, Failure to comply may result in legal penalties or reputational damage.

Security Awareness

Technology alone cannot stop all cyber attacks.

Employees should learn: How to identify phishing emails. How to create strong passwords. Why software updates are important. How to report security incidents? Regular awareness training helps reduce human errors.

Security Audits

Definition: A security audit is a systematic review of an organization's security controls to verify that they are working as intended.

Example

An auditor checks: Are passwords strong? Is antivirus installed? Are software updates applied? Are backups available? Are security policies being followed?

Summary

- **Governance** ensures that cyber security is planned, managed, and monitored effectively.
- It defines **who is responsible, what rules must be followed, and how security supports organizational goals.**
- Policies, standards, procedures, and guidelines work together to create a consistent security program.
- Risk management, compliance, awareness, and audits are key parts of good governance.

- Effective governance is not just the responsibility of the IT team—it requires participation from management, employees, and all users.

Key Terms

Term	Meaning
Governance	Directing and managing an organization
Security Policy	High-level security rules
Standard	Mandatory technical requirement
Procedure	Step-by-step instructions
Guideline	Recommended best practice
Risk	Possibility of harm or loss
Compliance	Following applicable rules and regulations
Audit	Review of security controls and processes

CIA Triad (Confidentiality, Integrity, and Availability)

The **CIA Triad** is one of the **most important concepts in Cyber Security**.

Almost every security system is designed to protect these three goals:

1. **Confidentiality (C)**

2. **Integrity (I)**

3. **Availability (A)**

If any one of these three is lost, the system may no longer be secure.

Simple Example

Imagine a **school examination paper**.

- Only teachers should see it before the exam. → **Confidentiality**
- Nobody should change the questions. → **Integrity**
- The paper should be available on exam day. → **Availability**

All three are important.

What is the CIA Triad?

The **CIA Triad** is a security model that ensures information is:

- **Confidential**
- **Accurate**
- **Available when needed**

Confidentiality

Definition: Confidentiality means that information is accessible **only to authorized people**.

Simple Definition

Only the right people should be able to see the information.

Example: Your bank account details should only be visible to: You and Authorized bank employees

A stranger should not be able to access them.

How to Maintain Confidentiality?

Organizations use many methods. Passwords, Multi-Factor Authentication (MFA), Encryption, Access Control, Data Classification.

Threats to Confidentiality: Confidentiality may be lost because of: Hacking, Phishing, Weak passwords, Insider misuse, Lost laptops, Stolen mobile phones, Misconfigured cloud storage

Integrity: Integrity means that information remains accurate, complete, and unaltered unless changed by an authorized person.

Simple Definition: Information should **not be changed incorrectly or without permission.**

How to Maintain Integrity?: Hashing, Digital Signatures, File Permissions, Backups, Version Control, Threats to Integrity.

Availability

Availability means that information and systems are accessible to authorized users whenever they are needed.

Simple Definition: The system should be working when users need it.

How to Maintain Availability? Regular Backups, Redundant Systems, Uninterruptible , Power Supply (UPS), Disaster Recovery Plan, System Monitoring.

Administrators monitor systems to detect problems quickly.

Threats to Availability

Examples include: Hardware failure, Power outage, Flood, Fire, DDoS attacks, Ransomware, Network failures.

Relationship Between the Three

All three work together. If one fails, security is weakened.

Comparison Table

Confidentiality	Integrity	Availability
Protects secrecy	Protects accuracy	Protects accessibility
Prevents unauthorized viewing	Prevents unauthorized changes	Prevents service interruption
Uses passwords, encryption, access control	Uses hashing, digital signatures, permissions	Uses backups, redundancy, monitoring

Important Keywords

Term	Meaning
Confidentiality	Preventing unauthorized access to information
Integrity	Keeping information accurate and unchanged unless authorized
Availability	Ensuring systems and data are accessible when needed
Encryption	Protecting data by converting it into a secure format
Hashing	Creating a fixed-length value to detect changes
Backup	A copy of data used for recovery
Access Control	Restricting access to authorized users only

Security Principles

Cyber Security is not only about using antivirus software or firewalls.

To build a secure system, organizations follow certain **Security Principles**.

These principles act as **guidelines** for designing, implementing, and maintaining secure systems.

Think of security principles as **traffic rules** for cyber security.

Just as traffic rules reduce accidents, security principles reduce cyber attacks.

What are Security Principles?

Security Principles are basic rules and best practices that help protect information, systems, and networks from cyber threats.

Simple Definition

Security principles are **rules that help make computer systems safe**.

Why are Security Principles Important?

They help organizations: Protect sensitive information, Reduce cyber-attacks, Control user access, Detect security problems, Recover from failures, Build reliable systems, Maintain customer trust.

Principle of Least Privilege (PoLP)

Definition: A user should receive **only the minimum permissions** needed to perform their job.

Simple Definition: Give only the permissions that are necessary—nothing more.

Example

In a college:

Student Can View marks Download assignments

Cannot: Change marks, Delete student records

Teacher Can Enter marks and Update attendance

Cannot Change payroll information

IT Administrator Can Manage servers, Create user accounts

Each person receives only the permissions required for their role.

Benefits: Reduces accidental mistakes, Prevents misuse, Limits damage if an account is compromised, Improves security

Real-Life Example: A cashier in a bank can process transactions but cannot approve large loans.

This follows the **Principle of Least Privilege**.

Need-to-Know Principle

Definition: Users should access information **only if they need it to perform their work**.

Example A doctor can access a patient's medical records.

A receptionist may only need the patient's appointment details, not their full medical history.

Difference Between PoLP and Need-to-Know

Least Privilege	Need-to-Know
Limits system permissions	Limits access to information
Focuses on what users can do	Focuses on what users can see

Separation of Duties (SoD)

Definition: Important tasks should be divided among different people.

No single person should control the entire process.

Example

In a company: Employee A creates a payment request. Employee B approves the payment. Employee C completes the payment.

Why? This reduces fraud and mistakes.

Banking Example

One employee should not: Create a customer account, Approve the account, Transfer money

All three tasks should be handled by different people.

Benefits: Prevents fraud, Reduces insider threats, Improves accountability.

Defense in Depth

Definition: Use **multiple layers of security** instead of relying on a single protection.

Simple Definition If one security layer fails, another layer still protects the system.

Example A company uses: Firewall, Antivirus, Strong passwords, Multi-Factor Authentication (MFA), Encryption, Security monitoring

Even if one layer fails, the others continue to provide protection.

Zero Trust Principle

Definition: Never trust automatically. Always verify.

Simple Definition Every user and device must prove their identity before receiving access.

Traditional Security Once a user enters the office network, they may be trusted automatically.

Zero Trust Every access request is verified, even if it comes from inside the organization.

Example

An employee logs into the company network.

The system asks for: Username, Password, OTP, Device verification

Only after successful verification is access granted.

Benefits Reduces insider threats, Protects remote workers, Improves security

Fail-Safe Defaults

Definition Access should be **denied by default** unless permission is explicitly granted.

Example

A new employee joins a company.

Initially: No access to confidential files.

The manager approves only the required permissions.

Why? It is safer to start with no permissions than to accidentally give too many.

Complete Mediation

Definition Every request to access a resource should be checked before access is allowed.

Example

A student opens the college portal.

Every time they try to access marks or attendance, the system checks whether they are authorized.

Benefits Prevents unauthorized access, Stops permission misuse

Open Design

Definition: A security system should remain secure even if its design is publicly known.

The security should depend on **secret keys or passwords**, not on hiding how the system works.

Example Modern encryption algorithms (such as AES) are publicly known.

They remain secure because the **encryption key** is secret.

Benefits: Allows experts to review and improve the design, Encourages stronger, well-tested security

Economy of Mechanism

Definition Security systems should be as simple as possible.

Simple systems are easier to understand, test, and maintain.

Example A login system with a straightforward design is often easier to secure than one with unnecessary complexity.

Benefits: Fewer mistakes, Easier maintenance, Easier security testing

Psychological Acceptability

Definition: Security should be easy for users to understand and use.

If security is too difficult, users may avoid it or find unsafe shortcuts.

Example: Using a fingerprint sensor is easier than entering a long password every few minutes.

People are more likely to use security correctly when it is convenient.

Benefits: Better user experience, Higher compliance, Fewer user errors

Security by Design

Definition: Security should be included **from the beginning** of system development, not added later.

Example: When developing an online shopping website:

Instead of launching first and adding security later, developers include: Secure login, Input validation, Encryption, Logging, Access control, during development.

Security by Default

Definition Systems should be secure immediately after installation.

Users should not have to enable important security features manually.

Example: A new Wi-Fi router comes with:

- . Default administrator password that must be changed during setup
- . WPA2 or WPA3 encryption enabled
- . Firewall enabled

Quick Revision Table

Principle	Meaning	Example
Least Privilege	Minimum required permissions	Student cannot edit marks
Need-to-Know	Access only necessary information	Receptionist cannot view medical history
Separation of Duties	Split critical tasks	One employee requests payment, another approves it
Defense in Depth	Multiple layers of protection	Firewall + Antivirus + MFA
Zero Trust	Always verify	Password + OTP for every login
Fail-Safe Defaults	Deny access unless allowed	New employee starts with no special permissions

Complete Mediation	Check every access request	Verify access each time a protected file is opened
Open Design	Security should not rely on secrecy of the design	Public encryption algorithm with a secret key
Economy of Mechanism	Keep security simple	Simple, well-designed login system
Psychological Acceptability	Make security easy to use	Fingerprint login
Security by Design	Build security from the start	Secure coding during software development
Security by Default	Secure settings enabled initially	Firewall enabled by default

Important Keywords

Term	Meaning
Least Privilege	Minimum permissions needed
Need-to-Know	Access only required information
Defense in Depth	Multiple security layers
Zero Trust	Verify every access request
Separation of Duties	Divide important tasks among different people
Access Control	Restrict access to authorized users
Security by Design	Include security from the beginning
Security by Default	Enable secure settings initially

Types of Security Controls

In cyber security, **threats cannot be completely removed.**

So we use **Security Controls** to reduce risk.

Think of security controls as **protective barriers** that help protect systems, data, and users.

Example

A bank protects money using:

- . Guards (physical control)
- . CCTV cameras (technical control)
- . Security rules for employees (administrative control)

All these together improve security.

What are Security Controls?

Definition: Security Controls are safeguards or countermeasures used to protect systems, networks, and data from cyber threats.

Security controls are **methods used to keep systems safe.**

Types of Security Controls (Main Classification)

Security controls are mainly divided into **three types:**

1. Administrative Controls
2. Technical Controls
3. Physical Controls

Administrative Controls

Definition: Administrative controls are **policies, rules, and procedures** created by an organization to manage security.

Administrative controls are **rules people must follow.**

Examples: Security policies. Employee training. Password policies. Incident response plans. Background checks. Access approval procedures

Real-Life Example A company policy says: Employees must change passwords every 90 days.

This is an **administrative control**.

Benefits: Improves awareness. Reduces human errors. Ensures consistent behaviour. Defines responsibilities

Technical Controls

Definition: Technical controls are **software or hardware-based security mechanisms** used to protect systems.

Technical controls are **tools and technology used for security**.

Examples: Firewalls, Antivirus software, Encryption, Multi-Factor Authentication (MFA), Intrusion Detection Systems (IDS), Access control systems, VPNs.

Real-Life Example

When you log into Gmail: Password verification, OTP (2FA), Encryption during login

These are **technical controls**.

Benefits: Automated protection. Fast response to threats. Reduces human dependency. Strong system-level security

Physical Controls

Definition Physical controls are **tangible security measures used to protect physical systems, devices, and facilities.**

Physical controls are **real-world protections like locks and guards.**

Examples

- Security guards, CCTV cameras, Biometric access (fingerprint/face scan), Locked server rooms, Door locks, Fire alarms, Security fences

Real-Life Example

A data center has: Fingerprint access. Security guards. CCTV monitoring
These prevent unauthorized physical access.

Benefits: Prevents physical theft, Protects hardware, Enhances facility security, Stops unauthorized entry

Comparison of Administrative, Technical, and Physical Controls

Type	Focus	Examples
Administrative	Rules and policies	Password policy, training
Technical	Technology-based protection	Firewall, encryption
Physical	Physical protection	Locks, CCTV, guards

Functional Classification of Security Controls

Security controls can also be classified based on their function:

- 1.Preventive Controls
- 2.Detective Controls
- 3.Corrective Controls
- 4.Deterrent Controls
- 5.Recovery Controls
- 6.Compensating Controls

Preventive Controls

Definition: Preventive controls are used to stop security incidents before they happen.

Preventive controls **prevent attacks.**

Examples: Strong passwords. Firewalls. Access control. Encryption. MFA. Security awareness training.

Example A firewall blocks unauthorized access attempts.

Detective Controls

Definition: Detective controls are used to **identify and detect security incidents when they occur.**

Detective controls find attacks.

Examples: Intrusion Detection System (IDS), Security logs, CCTV monitoring, Audit systems, Alerts and monitoring tools

Example: An IDS detects unusual login attempts and sends an alert.

Corrective Controls

Definition: Corrective controls are used to **fix problems after a security incident has occurred.**

Corrective controls **repair damage.**

Examples: System patching, Malware removal, Data restoration, System reconfiguration, Incident response actions

Example: A virus is removed using antivirus software and system is restored.

Deterrent Controls

Definition: Deterrent controls discourage attackers from attempting an attack.

Deterrent controls **discourage attacks**.

Examples: Warning signs (“Unauthorized access is prohibited”), Security cameras, Legal notices, Visible security guards

Example: A CCTV camera makes attackers think twice before attempting theft.

Recovery Controls

Definition: Recovery controls restore systems and data after an incident.

Recovery controls **bring systems back to normal.**

Examples: Backups, Disaster recovery plans, System restoration tools, Redundant servers

Example: A company restores data from backup after ransomware attack.

Compensating Controls

Definition: Compensating controls are **alternative security measures** used when primary controls cannot be implemented.

Compensating controls are **backup security methods.**

Examples: Using MFA when password policy cannot be enforced fully. Extra monitoring when encryption is not possible. Manual approval process instead of automated access control

Example: If a system does not support encryption, data is restricted using strict access control and monitoring.

Real-Life Example (Combined Controls)

Scenario: Online Banking System

Type	Control Used
Administrative	Password policy, user training
Technical	Encryption, firewall, MFA
Physical	Data center security, CCTV
Preventive	Firewall blocks attacks
Detective	IDS detects unusual activity

Corrective	System patching
Recovery	Backup restores data
Deterrent	Legal warnings
Compensating	Extra monitoring

Why Security Controls are Important?

Security controls help to: Prevent cyber attacks, Detect threats early, Reduce damage, Recover lost data, Protect sensitive information, Ensure system reliability, Maintain trust

Term	Meaning
Security Control	Measure to protect systems
Administrative Control	Rules and policies
Technical Control	Technology-based protection

Physical Control	Real-world protection
Preventive Control	Stops attacks
Detective Control	Detects attacks
Corrective Control	Fixes damage
Recovery Control	Restores systems
Deterrent Control	Discourages attacks
Compensating Control	Alternative control

Real-Life Cyber Attacks

A **cyber attack** is an attempt by hackers or cyber criminals to: Steal data, Damage, systems, Disrupt services, Gain unauthorized access, Demand money (ransom).

Cyber-attacks happen every day across the world.

They target: Individuals, Banks, Hospitals, Governments, Companies, Schools.

What is a Cyber Attack?

Definition: A **cyber attack** is a malicious attempt to damage, steal, or gain unauthorized access to computer systems, networks, or data.

A cyber attack is when **someone tries to hack or harm a computer system.**

Types of Real-Life Cyber Attacks

Phishing Attack: Phishing is a cyber attack where attackers send fake messages to steal personal information like passwords or bank details.

Example

You receive an email: “Your bank account is locked. Click here to verify your details.”

The link leads to a fake website that steals your password.

Real-Life Impact

- . Bank account theft
- . Identity theft
- . Data leakage

Prevention

- . Do not click unknown links
- . Check website URL carefully

- Never share OTP or password

Malware Attack: Malware is malicious software designed to damage or disrupt systems.

Types of Malware: Virus, Worm, Trojan, Spyware, Ransomware

Example

Downloading a cracked software installs a hidden virus that corrupts files.

Prevention

- Use antivirus. Download from trusted sources. Keep software updated

Ransomware Attack: Ransomware locks or encrypts your data and demands money to unlock it.

Example: A hospital system is locked, and attackers demand ₹50 lakh to restore access.

Real-Life Impact

- . Loss of critical data
- . Business shutdown
- . Financial loss

Prevention

- . Regular backups
- . Antivirus protection
- . Avoid suspicious downloads

Denial of Service (DoS)/Distributed DoS (DDoS)

A DDoS attack floods a system with huge traffic, making it unavailable to users.

Example: A shopping website crashes during a sale due to millions of fake requests.

Impact

- . Website downtime
- . Revenue loss
- . Customer dissatisfaction

Prevention

- . Firewall
- . Traffic filtering
- . Cloud-based protection

Man-in-the-Middle (MITM) Attack: An attacker secretly intercepts communication between two parties.

Example: A hacker intercepts your Wi-Fi connection and steals login credentials.

Prevention

- . Use HTTPS websites

- . Avoid public Wi-Fi for banking
- . Use VPN

Password Attack: Attackers try to guess or steal passwords.

Types

- . Brute force attack
- . Dictionary attack
- . Credential stuffing

Example: Using leaked passwords from one website to log into another account.

Prevention

- . Strong passwords
- . MFA (Multi-Factor Authentication)
- . Avoid password reuse

SQL Injection Attack: Attackers insert malicious SQL code into a website input field to access or modify database data.

Example: A login page is hacked to bypass authentication and access user data.

Impact

- . Data theft
- . Database corruption

Prevention

- . Input validation
- . Parameterized queries
- . Secure coding practices

Social Engineering Attack: Attackers manipulate people into giving sensitive information.

Example: A caller pretends to be a bank officer and asks for OTP.

Prevention

- Never share OTP or passwords
- Verify identity of callers
- Awareness training

Famous Real-Life Cyber Attacks

WannaCry Ransomware Attack (2017)

What Happened?

- A global ransomware attack infected computers in over 150 countries.
- It affected hospitals, businesses, and government systems.

Impact

- Hospital systems were shut down
- Critical data was locked

- . Huge financial losses

Lesson

Keep systems updated and use security patches.

Yahoo Data Breach

What Happened?

- . Millions of Yahoo user accounts were hacked.
- . Personal data and passwords were stolen.

Impact

- . Loss of user trust
- . Financial and legal issues

Lesson

Use strong encryption and secure password storage.

Equifax Breach (2017)

What Happened?

- . Credit reporting company Equifax was hacked.
- . Sensitive data of millions of users was exposed.

Impact

- . Identity theft risk
- . Financial losses

Lesson

Regular patching and vulnerability management are essential.

Facebook Data Leak (Cambridge Analytica)

What Happened?

- . User data was collected without proper consent.
- . Data used for political profiling.

Impact

- . Privacy violation
- . Public trust issues

Lesson

Strong privacy policies and data protection are required.

Impact of Cyber Attacks

Cyber attacks can cause: **Financial Loss, Data Loss, Reputation Damage, Service Disruption, Legal Consequences**

How Cyber Attacks Happen

Cyber attacks usually happen due to: Weak passwords, Unpatched software, Human mistakes, Phishing emails, Malware downloads, Poor security policies, Lack of awareness

How to Prevent Cyber Attacks: Use Strong Passwords, Enable MFA, Update Software Regularly, Use Antivirus and Firewalls, Be Careful with Emails, Regular Backups, Security Awareness Training.

Real-Life Example Summary Table

Attack Type	Example	Impact
Phishing	Fake bank email	Password theft
Ransomware	Locked hospital data	Financial loss
DDoS	Website crash	Service downtime
MITM	Wi-Fi interception	Data theft
SQL Injection	Database hack	Data breach

Malware	Virus download	System damage
---------	----------------	---------------

Exercise 1 – Identify Attack Type

Objective

Learn to recognize cyber attacks.

Task Match the scenario:

Scenario	Attack Type
Fake email asking for OTP	Phishing
Website crash due to traffic overload	DDoS
File locked and ransom demanded	Ransomware
Fake Wi-Fi stealing data	MITM
Virus from downloaded file	Malware

Key Terms

Term	Meaning
Cyber Attack	Attempt to damage or steal data
Malware	Malicious software
Phishing	Fake messages to steal data
Ransomware	Locks data and demands money
DDoS	Overloads a system with traffic
MITM	Intercepts communication
SQL Injection	Database attack
Social Engineering	Manipulating people to steal information