RV College of Engineering®

Go, change the world

22EM1C07-Introduction to Cyber Security

UNIT- I

Chapter-1: Introduction to Cyber Space

Text Book:

Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd, 1st Edition 2011,Reprint 2022, ISBN:978-81-265-2179-1.

Course Incharge: Dr.Mohana
Department of Computer Science & Engineering (Cyber Security)
RV College of Engineering, Bangalore-560059

Unit - I Syllabus

Unit-I	8 Hrs
Introduction to Cyber Space History of Internet, History and evolution of Information Security and cyber-Security, introduction to cyber space and information security, computer ethics and security policies. **Introduction to Cybercrime** Definition and Origins of the Word, Cybercrime and Information Security, who are Cybercriminals? Classifications of Cybercrimes, An Indian Perspective, Hacking and Indian Laws., Global Perspectives. Different Types of Cyber Crimes, Scams and Frauds	

Recent cyber attacks

EDITION IN | MANGALORE 25°C

THE TIMES OF INDIA

SUBSCRIB

India | Coronavirus Outbreak | Opinions And Features | Times Evoke | Maharashtra | Delhi | Karnataka | Tamil Nadu | Telangana | U

NEWS / INDIA NEWS / AIIMS Delhi Server Attack Originated From China, Say Government ...

AIIMS Delhi server attack originated from China, say government sources; data from 5 servers safely retrieved

ANI / Updated: Dec 14, 2022, 15:29 IST

46 PTS | SHARE | AA

ARTICLES

- AIIMS Delhi server attack originated from China, say government...
- Here's how IIM Calcutta's course in fintech and financial...
- Sharabi ho tum: Bihar CM Nitish Kumar screams at BJP MLAs in...
- 17 Opposition parties stage walkout from Rajya Sabha over...

NEW DELHI: The attack on the computer server of All India Institute of Medical

https://www.ndtv.com/topic/cyber-attacks

Cyber attacks

- Airports
- Railway tracks
- Metro station
- Power plant
- nuclear plant
- Toll plaza
- Datacenter
- Shopping mall
- Smart city
- Computers and internet

What is Cyber Security?

- Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

What is the Internet?

- Internet is an electronic communications network that connects computer networks and organizational computer facilities around the world.
- The internet is a globally connected network system facilitating worldwide communication and access to data resources through a vast collection of private, public, business, academic and government networks.
- Owners of Internet

Applications of Internet

1. Communication
2. Job searches
3. Finding books and study material
4. Health and medicine
5. Travel
6. Entertainment
7. Shopping
8. Stock market updates

Applications of Internet Contd..

9. Research

10. Business use of internet: different ways by which internet can be used for business are:

a. Information about the product can be provided can be provided online to the the customer .

b. Provide market information to the business

c. It help business to recruit talented people

d. Help in locating suppliers of the product

e. Fast information regarding customers view about companies product

f. Eliminate middle men and have a direct contact with contact with customer

g. Providing information to the investor by providing companies background and financial information on website.

History of Internet

- J.C.R. Licklider of MIT first proposed a global network of computers in 1962.
- The Internet was developed by Bob Kahn and Vint Cerf in the 1970s.
- No one person invented the internet. When networking technology was first developed, a number of scientists and engineers brought their research together to create the ARPANET.
- Advanced Research Projects Agency Network (ARPANET)

Timeline of the Internet

1969 — ARPAnet, the first version of the internet, is created and used to link computers at UCLA and Stanford.

1986 — NSFNET is founded, creating the backbone and providing the investment needed to create the internet as we know it today.

1989 — Tim Berners-Lee invents the world wide web, which opens the door for the internet to go mainstream.

1994 — Netscape navigator is released in stores.

2004 — Facebook launches and the Web 2.0 begins to grow rapidly.

2010 — 1.966 billion people are online worldwide.

1965 — Lawrence Roberts and Thomas Merril communicate with one another using computers connected via a low-speed dial-up telephone line in Massachusetts and California, creating the first Wide Area Network and laying the groundwork for the internet.

1974 — Robert Kahn and Vinto Cerf publish "A protocol for Packet Network Communication" laying the groundwork for TCP/IP and much larger, interconnected computer networks. The word "internet"is first used.

1989 — The first commercial ISP, the world launches.

1993 — The first web browser available to the public, Mosaic launches.

2000 — Some 300 million people around the world are officially online.

2007 — The iPhone is released, giving rise to the mobile revolution.

2022 — 5 billion people are online

HOW INTERNET WORKS?

- The Internet is a network of networks
- it connects to an Internet service provider (ISP).
- Many ISPs are big telecommunications companies.
- These providers connect to one another, exchanging traffic, and ensuring your messages can get to any other computer that's online and willing to communicate with you.
- The Internet was designed to be redundant and fault-tolerant—meaning that if one network, connecting wire, or server stops working, everything else should keep on running
- Available technologies have ranged from computer modems with acoustic couplers to telephone lines, to television cable (CATV), wireless Ethernet (wi-fi), and fiber optics.

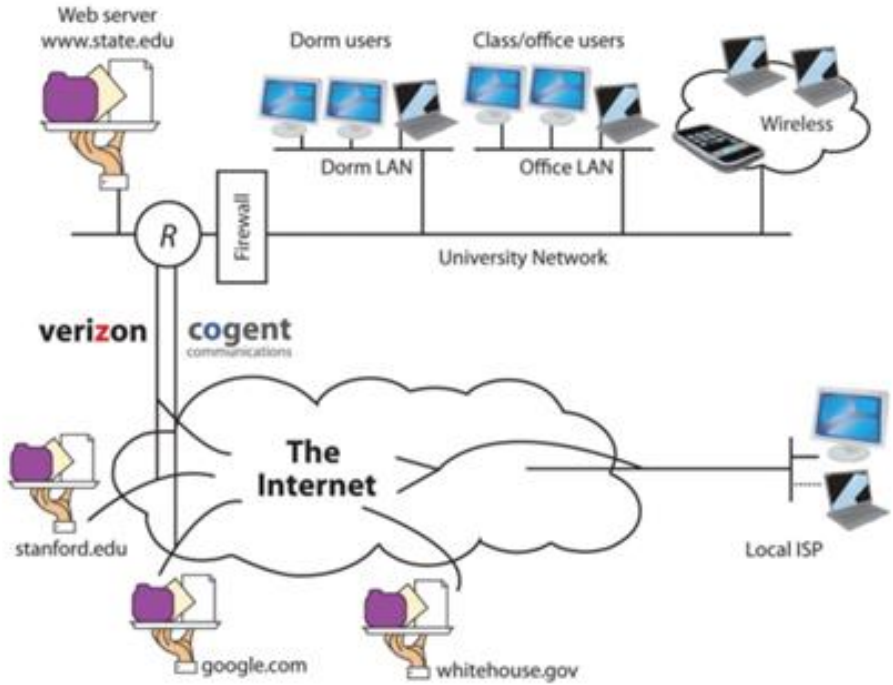


Figure: Working of the Internet

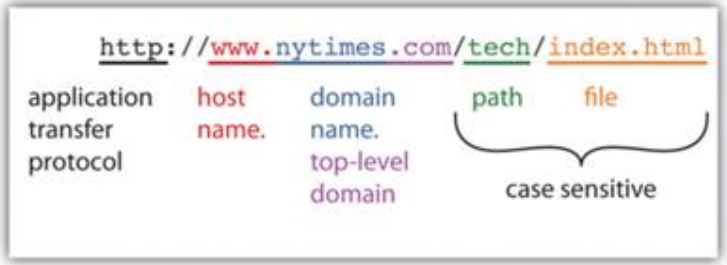


Figure: Anatomy of a Web Address

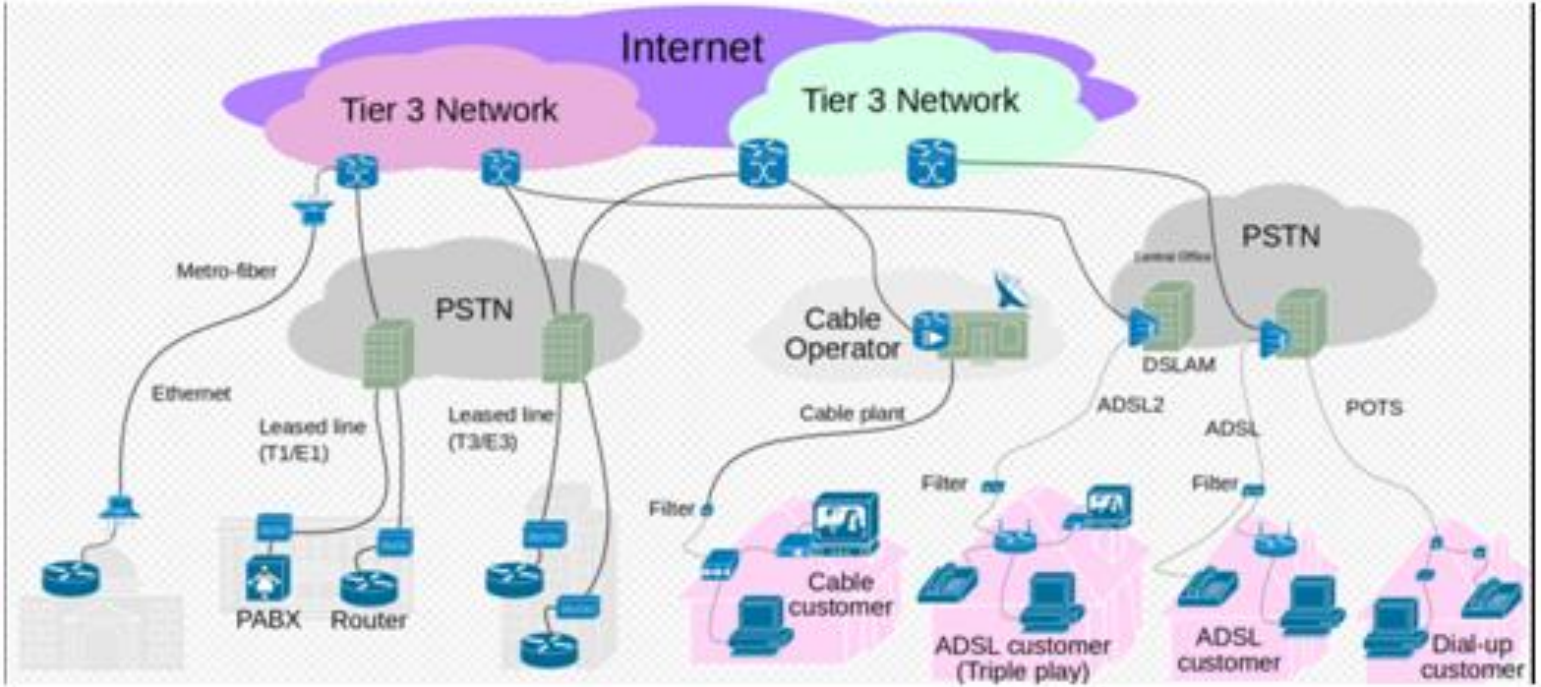
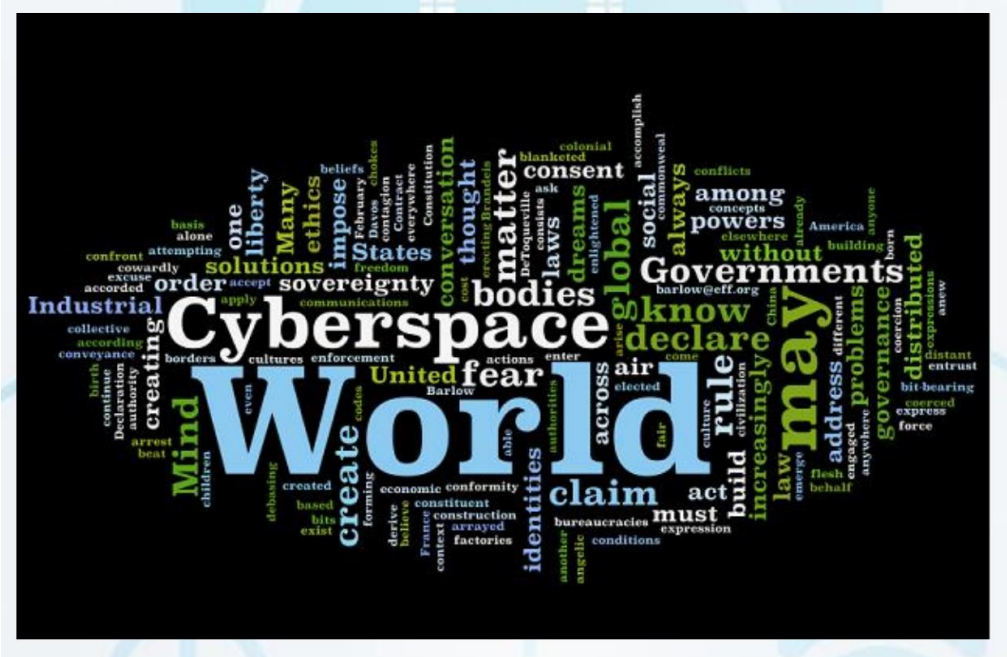


Figure: Internet connectivity options from end-user to tier 3/2 ISPs

Cyberspace- Definition

"Cyberspace refers to the **virtual space** that provides the **infrastructure, electronic medium** and **related elements** necessary for online global communication"



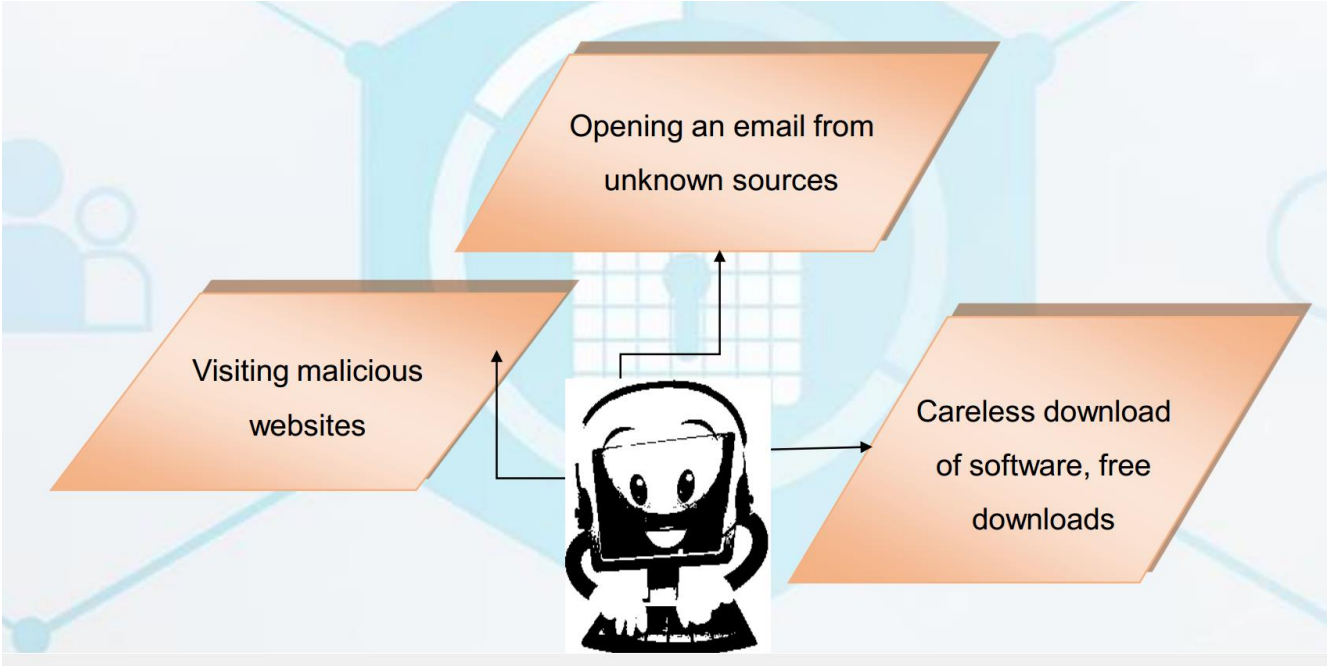
Why Cyber Security is important?

- Cyber Security is **not a one-time process** to achieve
- It is an **ever growing challenge** encountered from **time to time**
- When old problems are fixed and rectified, new targeted attacks challenge the Cyberspace
- Cyber security is a **process by itself and not the end**

Hackers

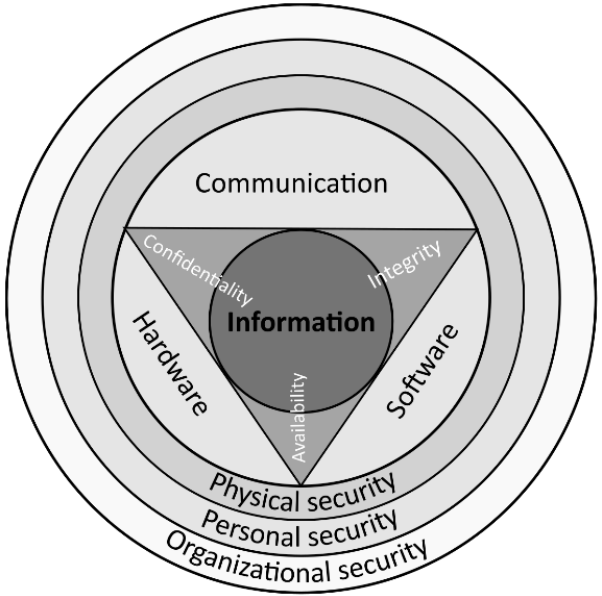
- Hackers are **unauthorized users** of a system.
- They invade a system through the vulnerabilities or weak points in the system.
- They makes use of large diverse tools to harm a computer system.
- They gain access to computer systems through malicious logic.

Common ways a computer can become infected:



Origin of information security

- In the 1970s, the true birth of cybersecurity began with a project called The Advanced Research Projects Agency Network (ARPANET).
- ARPANET was the network developed prior to the internet.



Principle of Information System Security: History

- Information security (IS) is designed to protect the confidentiality, integrity and availability of data from those with malicious intentions of misusing that data in many manners.
- **1960s: Offline sites security**
- **1970s: Evolution of personal computer and hackers**
- **1980s: Evolution of cyber-crime**
- **1990s: “Hacking” becoming an organized crime**
- **2000s: Cybercrime becoming a serious issue**
- **2010s: Information security**

Security System Development Life Cycle

- Security System Development Life Cycle (SecSDLC) is defined as the set of procedures that are executed in a sequence in the software development cycle (SDLC).
- System Investigation
- System Analysis
- Logical Design
- Physical Design
- Implementation
- Maintenance

Difference between Cyber Security and Information Security

- The terms **Cyber Security** and **Information Security** are often used interchangeably.
- As they both are responsible for the security and protecting the computer system from threats and information breaches.
- Cybersecurity and information security are so closely linked that they may seem synonymous and unfortunately, they are used synonymously.

Examples and Inclusion of Cyber Security:

- Network Security
- Application Security
- Cloud Security
- Critical Infrastructure

Examples and inclusion of Information Security:

- Procedural Controls
- Access Controls
- Technical Controls
- Compliance Controls

Parameters	CYBER SECURITY	INFORMATION SECURITY
Basic Definition	It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity, and availability.
Protect	It is about the ability to protect the use of cyberspace from cyber attacks.	It deals with the protection of data from any form of threat.
Scope	Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.
Threat	Cybersecurity deals with the danger in cyberspace.	Information security deals with the protection of data from any form of threat.
Attacks	Cybersecurity strikes against Cyber crimes, cyber frauds, and law enforcement.	Information security strikes against unauthorized access, disclosure modification, and disruption.
Professionals	Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).	Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and availability.
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.
Defense	Acts as first line of defense.	Comes into play when security is breached.

Network Security

- Network Security is the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems.
- This aims at securing the confidentiality and accessibility of the data and network.
- Every company or organization that handles a large amount of data, has a degree of solutions against many cyber threats.

Examples and inclusion of Network Security are:

- Firewall, Network Segmentation, Remote Access VPN, Email Security
- Intrusion Prevention Systems (IPS)Sandboxing
- Hyperscale Network Security.
- Data Loss Prevention (DLP)

Difference between Information Security and Network Security

Parameters	Information Security	Network Security
Data	It protects information from unauthorized users, access, and data modification.	It protects the data flowing over the network.
Part of	It is a superset of cyber security and network security.	It is a subset of cyber security.
Protection	Information security is for information irrespective of the realm.	It protects anything in the network realm.
Attack	It deals with the protection of data from any form of threat.	It deals with the protection from DOS attacks.
Scope	It strikes against unauthorized access, disclosure modification, and disruption.	Network Security strikes against trojans.
Usage	It provides confidentiality, integrity, and availability.	It provides security over the network only.
Ensures	Information security ensures to the protection of transit and stationary data.	Network security ensures to protect the transit data only.
Deals with	It deals with information assets and integrity, confidentiality, and availability.	It secures the data traveling across the network by terminals.

Computer Ethics

Commandments of Computer Ethics:

- not use a computer to harm other people.
- not interfere with other people's computer work.
- not snoop around in other people's computer files.
- not use a computer to steal.
- not use a computer to bear false witness.
- not copy or use proprietary software for which you have not paid (without permission).
- not use other people's computer resources without authorization or proper compensation.
- not appropriate other people's intellectual output.
- think about the social consequences of the program you are writing or the system you are designing.
- always use a computer in ways that ensure consideration and respect for other humans.

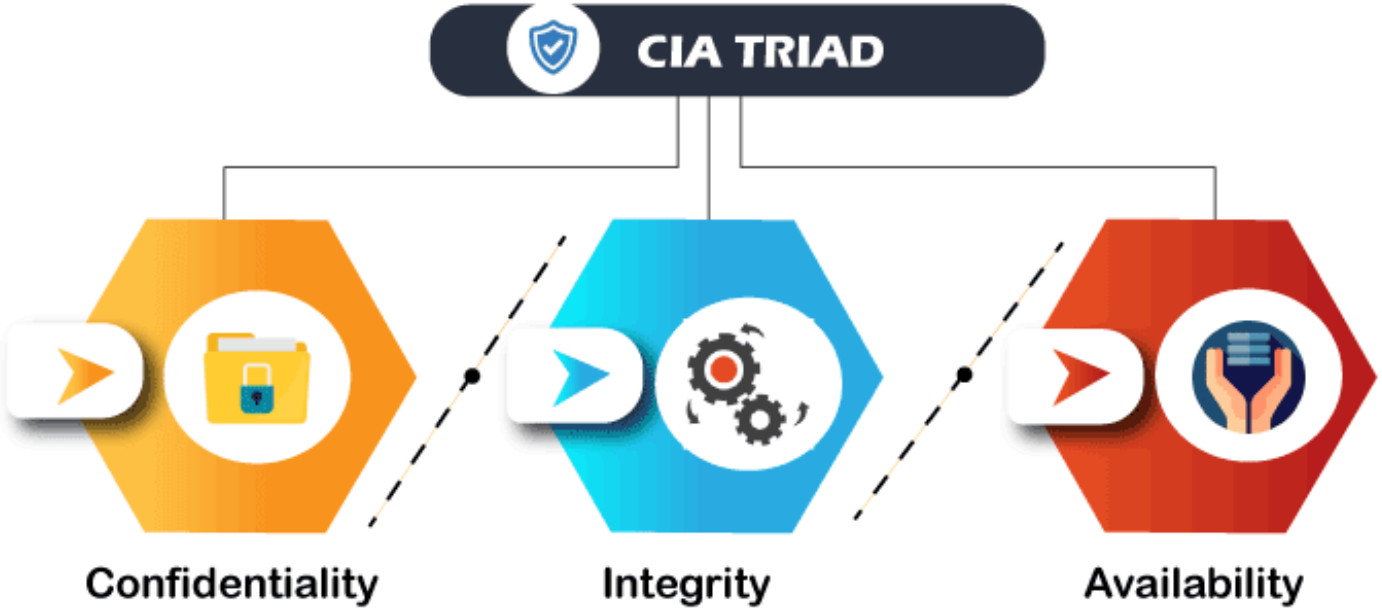
Definitions of cybersecurity

- Cybersecurity is the practice of protecting critical systems and sensitive information from **digital attacks.**
- **Cyber security** is the practice of **defending computers, servers, mobile devices, electronic systems, networks**, and **data from malicious attacks**.
- *"Cyber Security is the **body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access**."*
- *"Cyber Security is the **set of principles and practices designed to protect our computing resources and online information against threats**."*

Cyber Security Goals

- Main **objective is to ensure data protection**.
- Triangle of three related principles to protect the data from cyber-attacks.
- This principle is called the **CIA triad**.
- The CIA model is designed to guide policies for an organization's information security infrastructure. When any security breaches are found, one or more of these principles has been violated.
- **CIA model into three parts**: Confidentiality, Integrity, and Availability.
- It is actually a security model that helps people to think about various parts of IT security.

Cyber Security Goals



Confidentiality

- Privacy that avoids unauthorized access of information
- Ensuring the data is accessible by those who are allowed to use it and blocking access to others.
- It prevents essential information from reaching the wrong people.
- **Data encryption** is an excellent example of ensuring confidentiality.

Integrity

- Ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification.
- If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedily recover from such an event.
- In addition, it indicates to make the source of information genuine.

Availability

- Information to be available and useful for its authorized people always.
- accesses are not hindered by system malfunction or cyber-attacks.

Types of Cyber Security

- Network Security
- Application Security
- Information or Data Security
- Identity management
- Operational Security
- Mobile Security
- Cloud Security
- Disaster Recovery and Business Continuity Planning
- User Education

Network Security:

- Hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse.
- Protect its assets against external and internal threats.

Application Security:

- Protecting the software and devices
- Constantly updating the apps
- Design stage, writing source code, validation, threat modelling, etc., before a program or device is deployed

Information or Data Security:

- strong data storage mechanism to maintain the integrity and privacy of data

Identity management:

- procedure for determining the level of access that each individual has within an organization

Operational Security:

- making decisions on handling and securing data assets.

Mobile Security:

- cell phones, computers, tablets, and other similar devices against various malicious threats.

Cloud Security:

- protecting the information stored in the digital environment or cloud architectures for the organization.
- various cloud service providers such as AWS, Azure, Google, etc.

Disaster Recovery and Business Continuity Planning:

- processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data.

User Education:

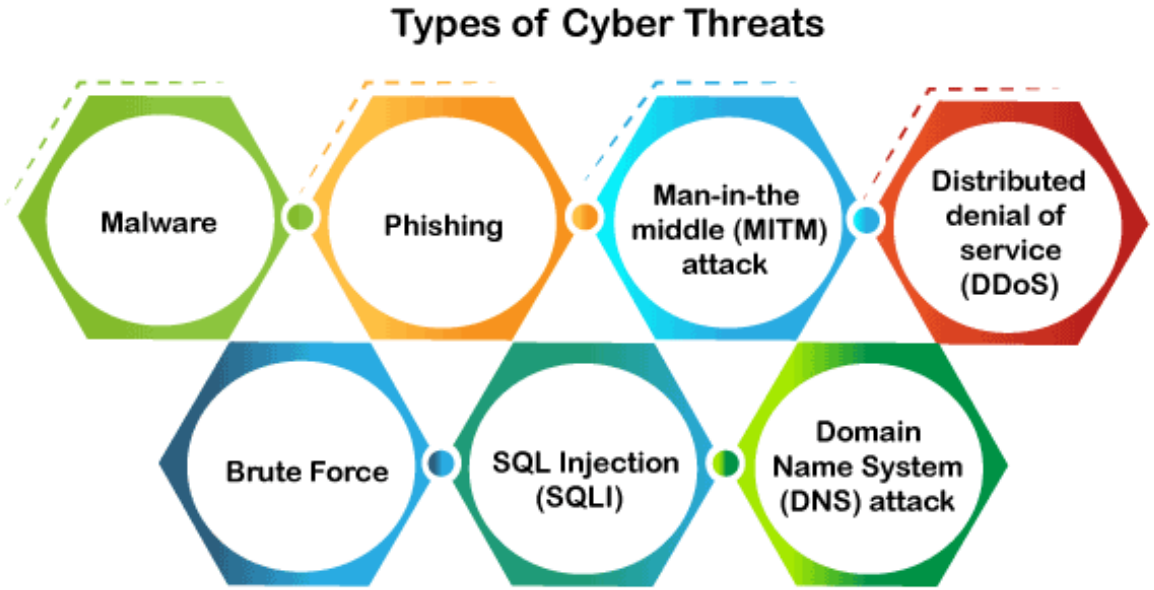
- the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data.

Why is Cyber Security important?

- All critical infrastructure such as the banking system, healthcare, financial institutions, governments, and manufacturing industries use **devices connected to the Internet** as a core part of their operations.
- Cyber-attack is now an international concern that hacks the system, and other security attacks could endanger the global economy.
- to **protect sensitive information** from **high-profile security breaches**.
- cyber-attacks grows, companies and organizations, especially those that deal with information related to **national security, health, or financial records, need to use strong cybersecurity measures and processes** to protect their sensitive business and personal information.

Types of Cyber Security Threats

- A threat in cybersecurity is a malicious activity by an individual or organization to corrupt or steal data, gain access to a network, or disrupts digital life in general.



Malware

- Malicious software, most common cyber attacking tool.

Virus: spreads from one device to another.

Spyware: secretly records information about user activities

- Ex. capture credit card details that can be used by the cybercriminals for unauthorized shopping, money withdrawing, etc.

Trojans: fool us into downloading and running.

- to corrupt or steal data from our device or do other harmful activities on our network

Ransomware: encrypts a user's files and data on a device

Worms: spreads copies of itself from device to device without human interaction data.

Adware: advertising software used to spread malware and displays advertisements on our device.

- unwanted program that is installed without the user's permission.
- generate revenue for its developer by showing the ads on their browser.

Botnets: collection of internet-connected malware-infected devices that allow cybercriminals to control them.

- It enables cybercriminals to get credentials leaks, unauthorized access, and data theft without the user's permission.

Phishing:

- **sender seems to come from a genuine organization** like PayPal, eBay, financial institutions, or friends and co-workers
- This link will redirect them to fraudulent websites to provide sensitive data such as personal information, banking and credit card information, social security numbers, usernames, and passwords.

Man-in-the-middle (MITM) attack:

- intercepts a conversation or data transfer between two individuals

Distributed denial of service (DDoS):

- cybercriminals disrupt targeted servers, services, or network's regular traffic by fulfilling legitimate requests to the target or its surrounding infrastructure with Internet traffic.

Brute Force:

- cryptographic hack that uses a trial-and-error method

SQL Injection (SQLI):

- malicious SQL scripts for backend database manipulation to access sensitive information.

Domain Name System (DNS) attack

- cyber criminals take advantage of flaws in the Domain Name System to redirect site users to malicious websites (DNS hijacking) and steal data from affected computers.

system affected by security breaches and attacks

Communication: Cyber attackers can use phone calls, emails, text messages, and messaging apps for cyberattacks.

Finance: risk of financial information like bank and credit card detail. This information is naturally a primary target for cyber attackers.

Governments: The cybercriminal generally targets the government institutions to get confidential public data or private citizen information.

Transportation: In this system, cybercriminals generally target connected cars, traffic control systems, and smart road infrastructure.

Healthcare: A cybercriminal targets the healthcare system to get the information stored at a local clinic to critical care systems at a national hospital.

Education: A cybercriminals target educational institutions to get their confidential research data and information of students and employees**.**

Benefits of cybersecurity

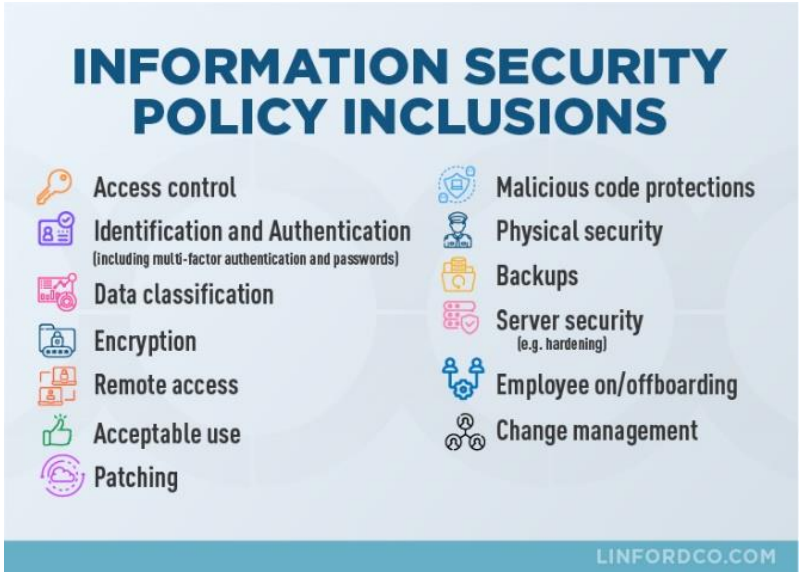
- Cyberattacks and data breach protection for businesses.
- Data and network security are both protected.
- Unauthorized user access is avoided.
- After a breach, there is a faster recovery time.
- End-user and endpoint device protection.
- Regulatory adherence.
- Continuity of operations.
- Developers, partners, consumers, stakeholders, and workers have more faith in the company's reputation and trust.

Cyber Safety Tips

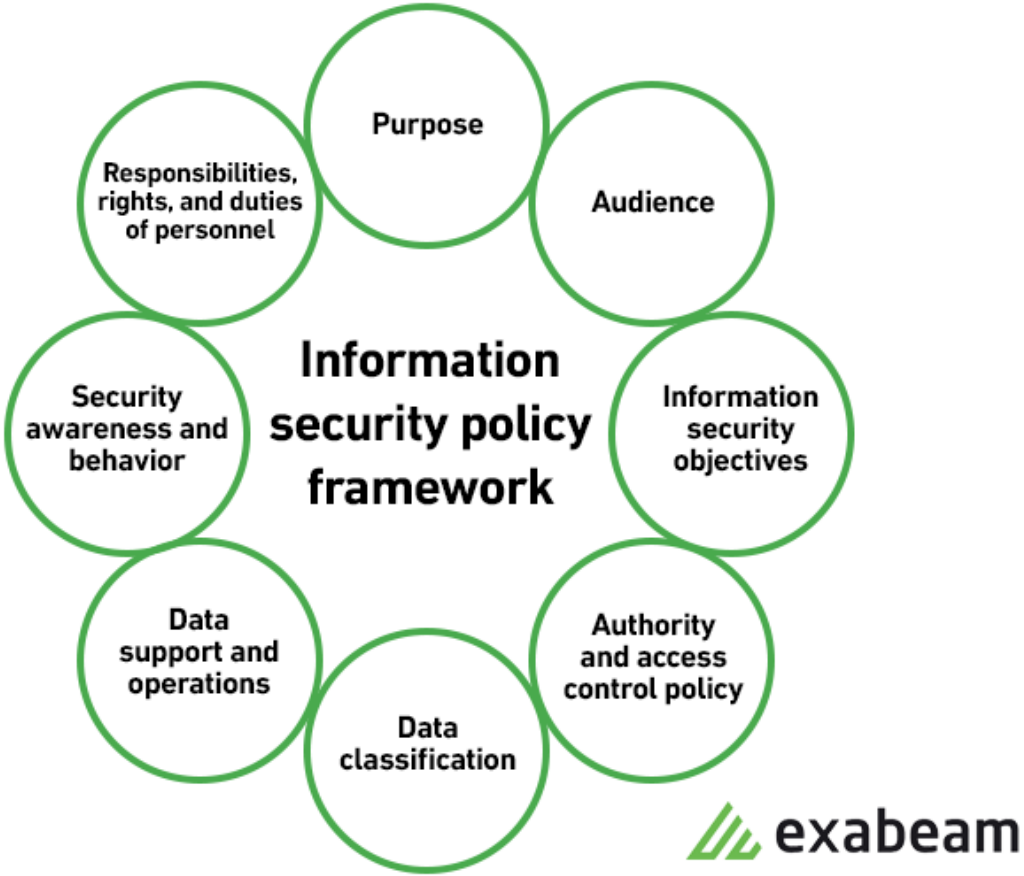
- Conduct cybersecurity training and awareness
- Update software and operating system
- Use anti-virus software
- Perform periodic security reviews
- Use strong passwords
- Do not open email attachments from unknown senders
- Avoid using unsecured Wi-Fi networks in public places
- Backup data

Security Policies

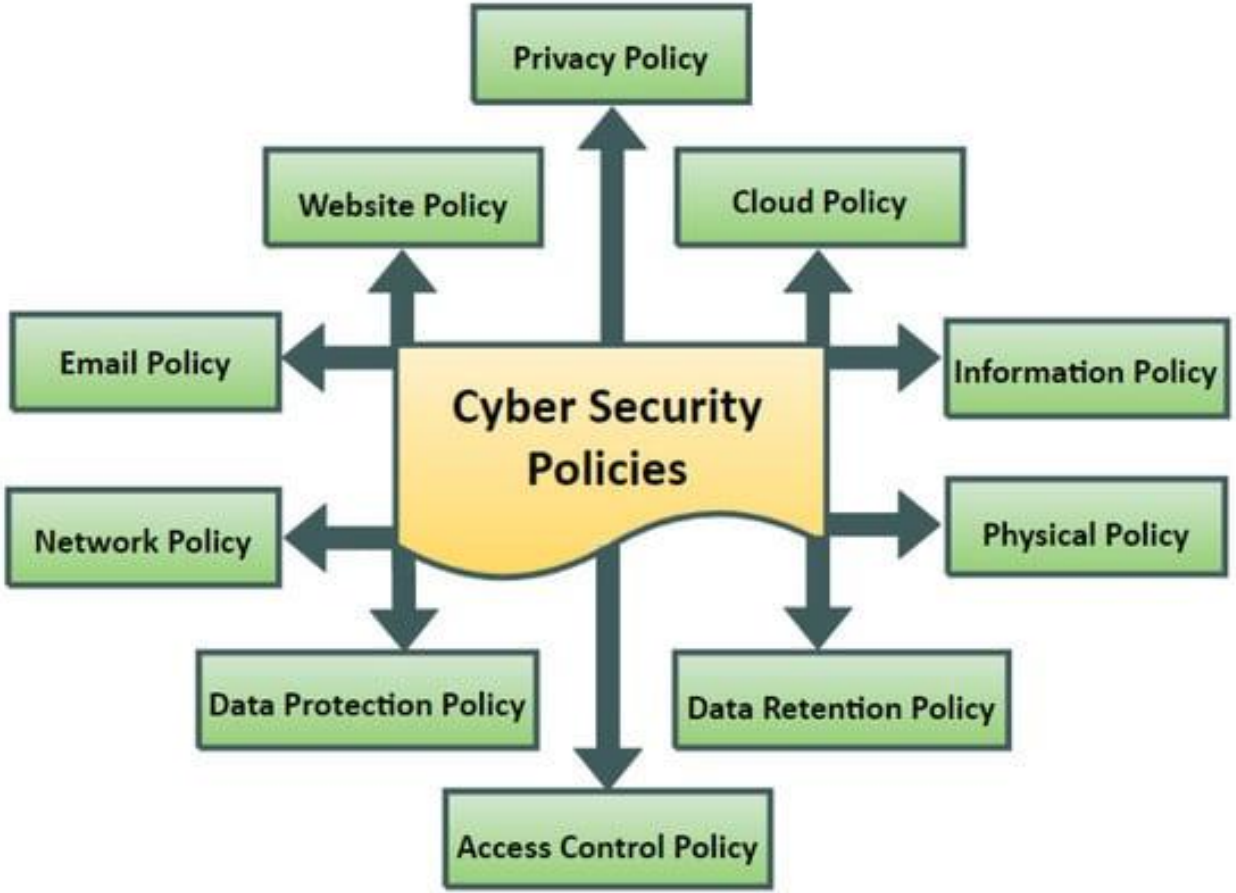
- A security policy (information security policy or IT security policy)
- Document Spells out the rules, expectations, and overall approach that an organization uses to maintain the confidentiality, integrity, and availability of its data.
- **technical security and administrative security policies**.
- Technical security policies describe the configuration of the technology for convenient use; body security policies address however all persons should behave.


INFORMATION SECURITY POLICY INCLUSIONS
Access control
Identification and Authentication
(including multi-factor authentication and passwords)
Data classification
Encryption
Remote access
Acceptable use
Patching
Malicious code protections
Physical security
Backups
Server security
(e.g. hardening)
Employee on/offboarding
Change management
LINFORDCO.COM


Cyber Security Policies
Intrusion Prevention Policy
LiveUpdate Policy
Application and Device Control
Exceptions Policy
Host Integrity Policy
Access Control Policy
Change Management Policy
Information Security Policy


Purpose
Audience
Information security objectives
Authority and access control policy
Data classification
Data support and operations
Security awareness and behavior
Responsibilities, rights, and duties of personnel
Information security policy framework
exabeam


Identify assets
Evaluate Threats & Risk
Apply safeguards
Monitor Safeguards
Respond to security incidents
Make Adjustment
Cyber Security Cycle


Privacy Policy
Website Policy
Cloud Policy
Email Policy
Cyber Security Policies
Information Policy
Network Policy
Physical Policy
Data Protection Policy
Data Retention Policy
Access Control Policy

Thank you