Faculty of Computer Applications &
Information Technology

BCA Programme

210301502

INFORMATION SECURITY

Unit -1 Introduction to IS and Need for the Security

- **Introduction to Information Security**
  - What is Security
  - Types of Security
  - Key Information Security Components
  - Critical Characteristics of Information
  - Components of Information System
  - Security Professionals and the Organization
- **Need of Information Security**
  - Threats (Overview)
    - Security Attacks (Overview)

UNIT -1 Inroduction to IS

- **What is “INFORMATION”?**
  - Information is **organized or classified data**, which has some meaningful values for the receiver.
  - Information is the **processed data** on which decisions and actions are based.

- **What is “SECURITY”?**
  - “The **Quality or state of being secure** – to be free from danger”
  - “**Protection against adversaries** – from those who would do harm, intentionally or other wise”

UNIT -1 Inroduction to IS

What is “INFORMATION SECURITY”?

- Information Security is not only about securing information from unauthorized access.
- Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
- It has many areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc
- **During First World War, Multi-tier Classification System was developed keeping in mind sensitivity of information. Alan Turing was the one who successfully decrypted Enigma Machine which was used by Germans to encrypt warfare data.**

UNIT -1 Types of Information Security

- A sucessful organization should have the following physical layers of security in place to protect its operations.
  - **Physical Security**
  - **Personnel Security**
  - **Operations Security**
  - **Communications Security**
  - **Network Security**
  - **Information Security**

UNIT -1 Types of Information Security

- A sucessful organization should have the following physical layers of security in place to protect its operations.

Physical Security

- To **protect physical items, objects or areas** from unauthorized access and misuse.
- Building, Computers, Files etc....

Personnel Security

- To **protect the individual or group of individuals** who are authorized to access the organization and its operations.
- Admin, User etc....

UNIT -1 Types of Information Security

- A successful organization should have the following physical layers of security in place to protect its operations.

Operations Security

- To **protect the details of a particular operations** or series of activities.
- Product Manufacturing secret.

Communications Security

- To protect **communications media, technology and content**
- Wired / Wireless media, storage media etc.

UNIT -1 Types of Information Security

- A successful organization should have the following physical layers of security in place to protect its operations.

Network Security

- To **protect networking components, connections and contents.**
- Network Devices and Packets of data etc...

UNIT -1 Types of Information Security

- A successful organization should have the following physical layers of security in place to protect its operations.

Information Security

- To protect the **(CIA / AIC)**
  - **Confidentiality**
  - **Integrity and**
  - **Availability**
  - of information assets.
- The assets whether in **storage, processing or transmission**

UNIT -1 Types of Information Security

Confidentiality

- Confidentiality is roughly **equivalent to privacy**. Measures undertaken to ensure confidentiality are designed to **prevent sensitive information from reaching the wrong people,** while **making sure that the right people can in fact get it.**
- In other words , A system's ability to ensure that only the correct, authorized user/system/resource can view, access, change, or otherwise use data

Integrity

- Integrity involves **maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle**. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.
- A system's ability to ensure that the system and information is accurate and correct.

UNIT -1 Types of Information Security

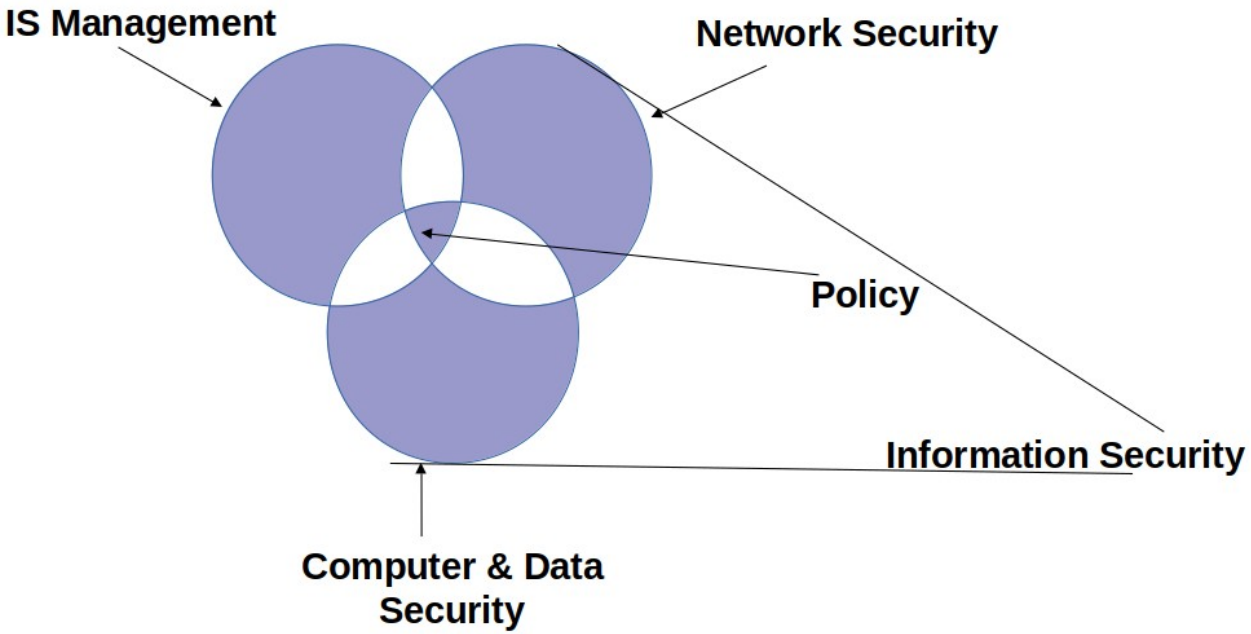
Availability

- Availability of information refers to ensuring that **authorized parties are able to access the information when needed.**
- Information only has **value if the right people can access it at the right times.**
- A system's ability to ensure that systems, information, and services are available the vast majority of time.

UNIT -1 IS BY CNSS

- The CNSS (Committee on National Security Systems) defines information security as ***the protection of Information and its critical elements, including the systems and hardware that use, store and transmit the informations.***
- ***IS*** *includes the broad areas of*
  - **IS Management**
  - **Computer and Data Security**
  - **Network Security**

UNIT -1 IS BY CNSS



UNIT -1 IS BY CNSS

- The **CNSS Model** of IS evolved from a computer security industry and **called C.I.A Triangle**.
- The **C.I.A triangle has been the industry standard for computer security** since development of the mainframe.
- The **C.I.A triangle based on three characteristics** of information
  - Confidentiality
  - Integrity
  - Availability

UNIT -1 Critical Characteristics of Information

- Availability
  - Availability enables **authorized users – persons or computer systems – to access information without interference or obstruction** and to receive it in the **required format.**
- Accuracy
  - Information h**as accuracy when it is free from mistakes or errors** and it has the value that the end user expects.
- Authenticity
  - Authenticity of information is the **quality or state of being genuine or original,** rather than a reproduction or fabrication.
  - Information is authentic when **it is the same state in which it was created, placed, stored or tranferred**.

UNIT -1 Critical Characteristics of Information

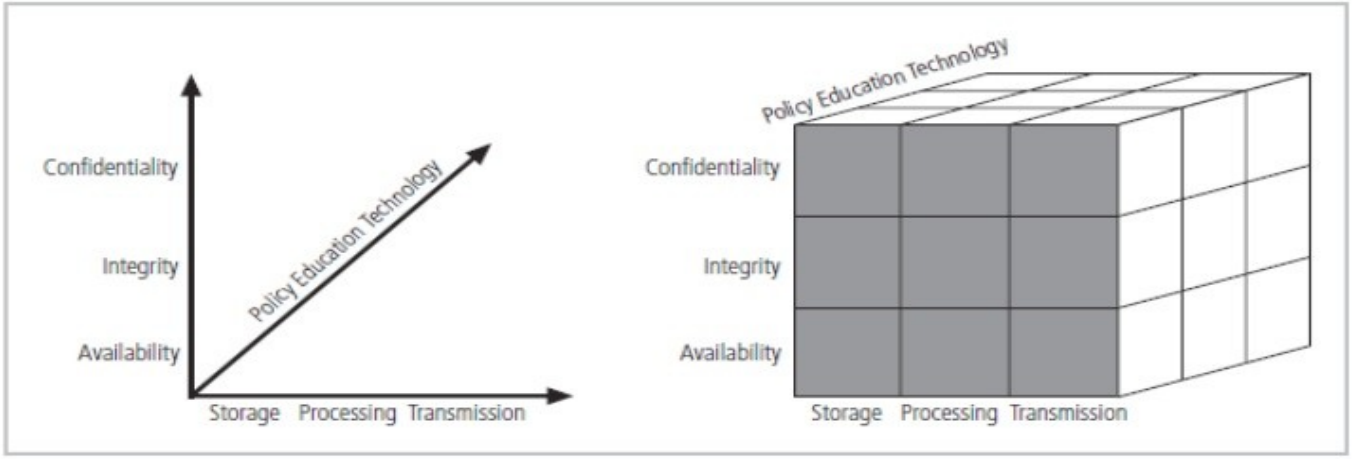
- Confidetiality
  - Information has confidentiality when **it is protected from disclosure or exposure to unauthorized** individuals or systems.
  - It insured that **only those with the rights and privileges to access information** are able to do so.
  - To protect the confidentiality of information, we can use number of mesures like:
  - Information classification
  - Secure document storage
  - Application of general security policies
  - Education of information custodians and end users.

UNIT -1 Critical Characteristics of Information

- Integrity
  - Information has integrity when it i**s whole, complete and uncorrupted.**
- Utility
  - The **utility of information is the quality or state of having value** for some purpose. **Information has value when it can serve a purpose.**
- Possession
  - **The possession of information is the quality or state of ownership or control.**
  - Information is said to be **one's possession if one obtains it, independent of format or other characteristics.**

UNIT -1 CNSS Security Model

CNSS Security Model



The McCumber Cube

UNIT -1 Key Information Security Concepts

- Access
  - A subject or object's **ability to use, manipulate, modify or affect** another subject or object.
- Asset
  - The **Organizational resource** such
  - Logical (Website, Information, Data etc..)
  - Physical (Person, Computer etc..)

UNIT -1 Key Information Security Concepts

- Attack
  - An intentional or unintentional **act that can cause damge to or otherwise compromise information** and/or the sytem that support it.
    - Active Attack
    - Passive Attack
    - Intentional Attack
    - Unintentional Attack
    - Direct Attack
    - Indirect Attack

UNIT -1 Key Information Security Concepts

- Control, Safeguard or Countermeasure
  - **Security mechanisms, policies or procedures that can successfully counter attacks, reduce risk**, resolve vulnerabilities and **improve the security** within an organization.
- Exploit
  - A **technique used to compromise a system.** A threat agent may **attempt to exploit a system or other information** asset by using **it illegally** for their personal gain.

UNIT -1 Key Information Security Concepts

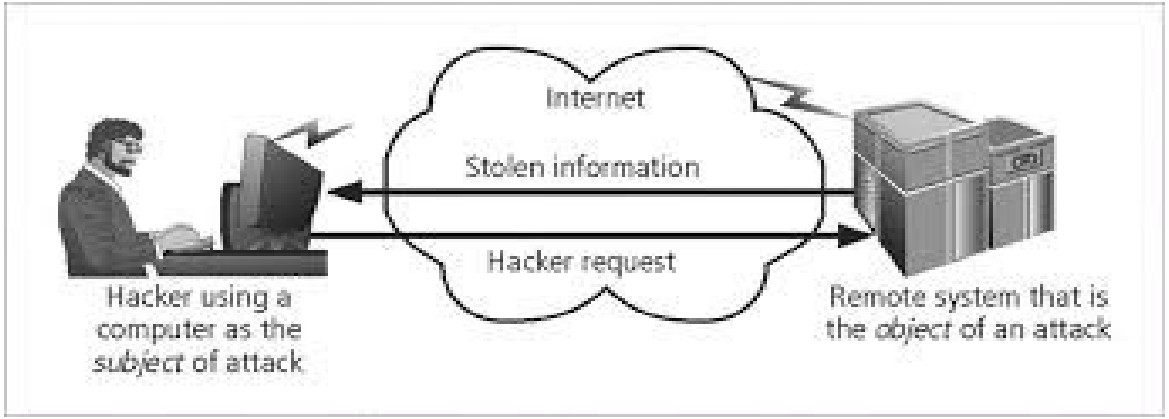
- Exposure
  - A condition or state of being exposed.
- Loss
  - **A single instance of an information asset suffering damage** or unintended or unauthorized modification or disclosure.
- Protection Profile or Security posture
  - The **entire set of controls and safefuards, including policy, education, training and awareness and technology that the organization implements to protecct the asset.**

UNIT -1 Key Information Security Concepts

- Risk
  - The **probability that something unwanted will happen**.
- Threat
  - A **category of objects, persons or other entities that presents a danger to an asset.**
- Threat Agent
  - The specific instance or a component of a threat.

UNIT -1 Key Information Security Concepts

- Subject and Objects
  - A computer can be either the subject of an attack or the object of an attack.



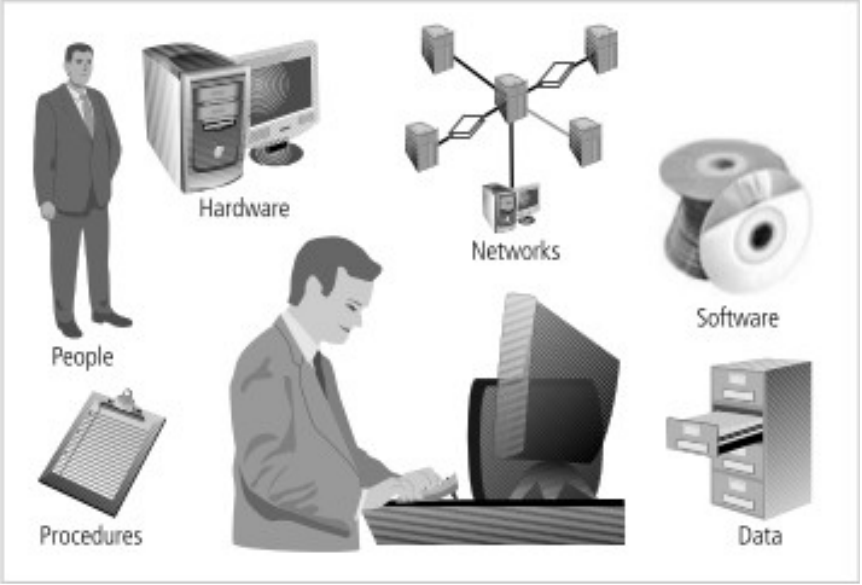
UNIT -1 Key Information Security Concepts

- Vulnerability
  - **A Weakness or fault in a system or protection mechanism** that opens it to attack or damage.

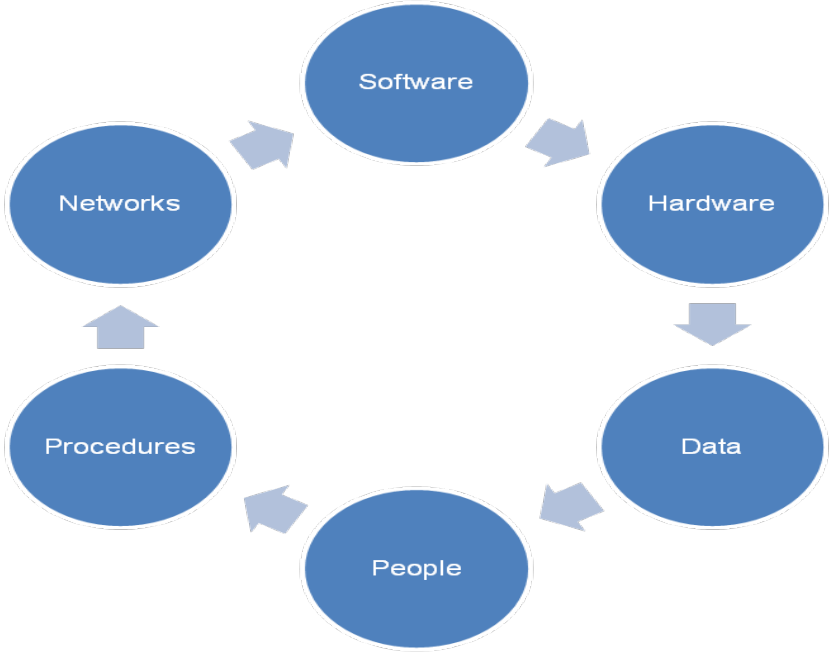
	Vulnerability	Threat	Risk
Example 1	Terminated employee ID's are not removed from the system	Dialing into the company's network and accessing proprietary info	Unauthorized disclosure of sensitive business information
Example 2	Improper maintenance of fire fighting equipment	Fire	Loss of life, data and infrastructure

UNIT -1 Components of IS

- IS is much more than computer hardware. It is the **entire set of software, hardware, data, people, procedures and networks** that make possible the use of information resources in the organization



UNIT -1 Components of IS



UNIT -1 Components of IS

- Software
  - The software component of the **IS comprises applications, operating systems and assorted command utilities**
  - Software is perhaps the **most difficult IS components to secure.**
  - The exploitation of errors in software programming accounts for a substantial portion of the attacks on information. The information technology industry is rife with reports warning of holes, bugs, weaknesses, or other fundamental problems in software.
  - Software carries the lifeblood of information through an organization.

UNIT -1 Components of IS

- Hardware
  - Hardware is t**he physical technology that houses and executes the software, stores and transports the data and provides interfaces for the entry and removal of information from the system.**
  - Physical security policies deal with hardware as a physical asset and with the **protection of physical assets form harm of theft.**
  - **Breach of Physical security can result in a loss of information.**
  - Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted access to the hardware is possible.

UNIT -1 Components of IS

- Data
  - Data s**tored, processed and transmitted by a computer system must be protected.**
  - Data is often the **most valuable asset possessed by an organization and it is the main target of intentional attacks.**
  - Systems developed in recent years are likely to make use of database.
  - When done properly, this should improve the security of the data and the application.
  - Unfortunately, many system development projects do not make full use of the database management system's security capabilities, and in some cases the database is implemented in ways that are less secure than traditional file systems.

UNIT -1 Components of IS

- People
  - Though often overlooked in computer security considerations, **people have always been a threat to information security.**
  - People can be the weakest link in an organization's information security program. And unless policy, education and training, awareness, and technology are properly employed to prevent people from accidentally or intentionally damaging or losing information, they will remain the weakest link.
  - Social engineering can prey on the tendency to cut corners and the common-place nature of human error.

UNIT -1 Components of IS

- Procedure
  - **Procedures are written instructions for accomplishing a specific task.**
  - When an **unauthorized user obtains an organization's procedures, this poses a threat to the integrity** of the information.
  - For example, a consultant to a bank learned how to wire funds by using the computer center’s procedures, which were readily available. By taking advantage of a security weakness (lack of authentication), this bank consultant ordered millions of dollars to be transferred by wire to his own account.

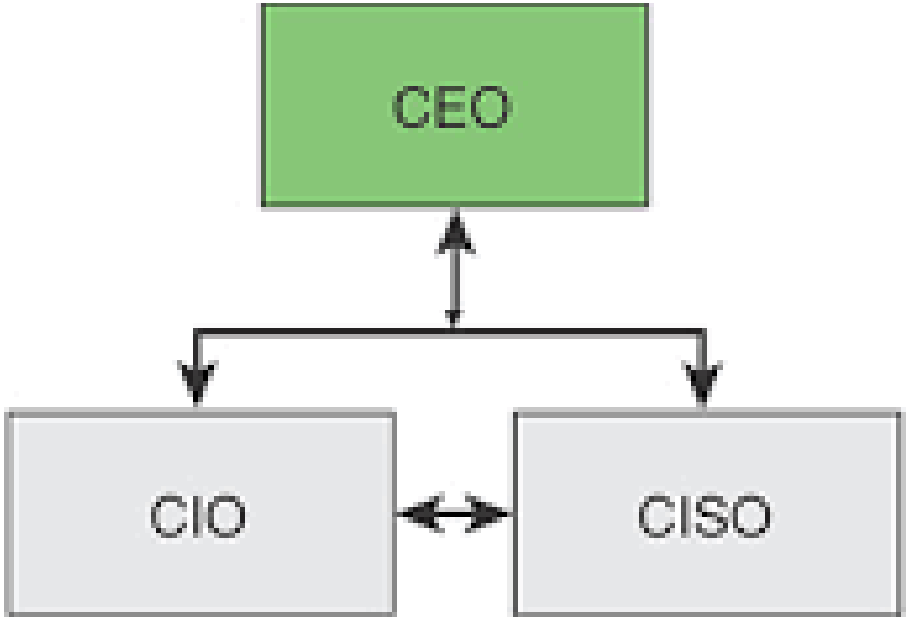
UNIT -1 Components of IS

- Networks
  - The IS component that created much of the need for increased computer and information security is networking.
  - When information systems are connected to each other to form local area networks (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge.
  - The physical technology that enables network functions is becoming more and more accessible to organizations of every size.
  - Applying the traditional tools of physical security, such as locks and keys, to restrict access to and interaction with the hardware components of an information system are still important; but when computer systems are networked, this approach is no longer enough.

UNIT -1 Security Professionals and the Organization

- **Senior Management** is the key component and the vital **force for a successful implementation of an IS Program**.
- Following professional has responsibilities of IS Program in a organization
  - Senior Management – Chief Information Officer (CIO)
  - Chief Information Security Officer (CISO)
  - Information Security Project Team Members
  - Data Responsibilities Members.

UNIT -1 Security Professionals and the Organization



UNIT -1 Security Professionals and the Organization

- **Senior Management**
  - The senior technology officer is typically the Chief Information Officer (CIO).
  - He / she also know as **Vice President of Information/** VP of Information Technology / VP of Systems.
  - **Responsibilities**
    - **CIO is primarily responsible** for **advising** the chief executive officer/ President **on the strategic planning that affects the management of Information** in the Organization.

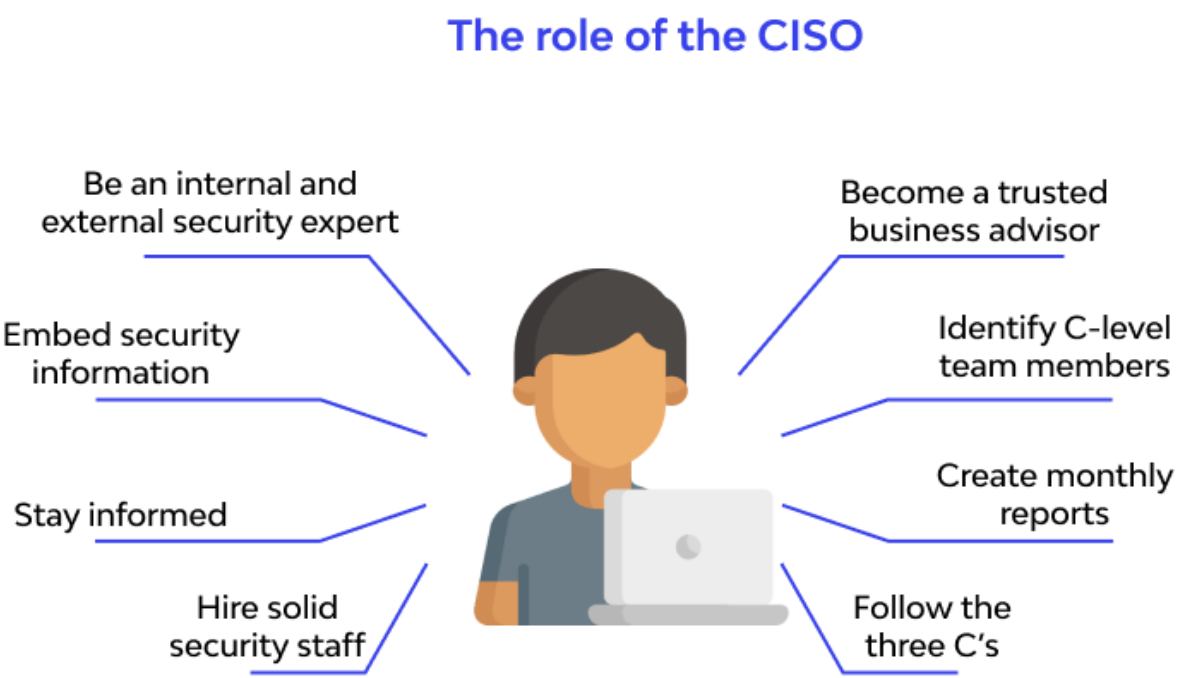
UNIT -1 Security Professionals and the Organization

- The **CIO translates the strategic plans** of the organization as a whole into strategic information plans for the **information systems or data processing division of the organization**.
- Once this is accomplished, CIOs work with subordinate managers to develop tactical and operational plans for the division and to enable planning and management of the systems that support the organization.

UNIT -1 Security Professionals and the Organization

- **Senior Management**
- **Chief Information Security Officer (CISO)**
  - He / she also **know as Manager of IT Security / Security administrator.**
  - Has primary **responisibility for the assessment, management and implementation of IS** in the organization.
  - The CISO usually reports directly to the CIO, although in larger organizations it is not uncommon for one or more layers of management to exist between the two.
  - However, the recommendations of the CISO to the CIO must be given equal, if not greater, priority than other technology and information-related proposals.

UNIT -1 Security Professionals and the Organization



UNIT -1 Security Professionals and the Organization

- **Information Security Project Team**
  - Team consist of **number of individuals whor are experienced in one or more facets** of the required technical and nontechnical areas.
  - **Champion**
    - A **senior executive who promotes the project** and ensures its support, both **financially and administratively.**
  - **Team Leader**
    - A project manager – **who understands project management, personnel management and IS technical requirement.**

UNIT -1 Security Professionals and the Organization

- **Information Security Project Team**
  - **Security Policy Developers**
    - People who **understand the organizational culture, exisiting policies,** and requirements for developing and implementing policies.
  - **Risk Assessment Specialists**
    - People **who understand financial risk assessment techniques**, the value of organizational assets and the security methods to be used.
  - **Security Professionals**
    - **Dedicated, trained and well educated specialists** in all aspectes of IS (Technical and Non technical)
  - **System Administrators**
    - **People with the primary responsibility for administering the system.**
  - **End Users**
    - **Those whom the new system will most directly affect.**

UNIT -1 Security Professionals and the Organization

- **Data Responsibilities**
  - **Data Owners**
    - Those **responsible for the security and use of a particular set of information.**
  - **Data Custodians**
    - Working directly with data owners, data custodians are **responsible for the storage, maintenance and protection of the information.**
  - **Data Users**
    - Who **work with the information to perform their assigned roles** supporting the mission of the organization.

UNIT -1 Threats

- To **protect your organization's i**nformation, you must know:
  - (1) yourself, that is be **familiar with the information to be protected** and the systems that store, transport and process it.
  - (2) **to know the threats you may face**
- **Threat is an object, person, or other entity that presents an ongoing danger to an asset.**

UNIT -1 Threats

- **Fourteen General categories** that represent clear and present dangers to an organization's people, information and systems.

  1. Compromises to Intellectual Property

  - Intellectual property is defined as “**the ownership of ideas and control over the tangible or virtual representations of those ideas”**
  - Intellectual Property can be **trade secrets, copyrights, trademarks and patents.**

UNIT -1 Threats

2. Deliberate Software Attacks

- It occurs when an **individual or group designs and deploys software to attack a system**.
- It also known as **malicious code / malicious software / malware.**
  - 2.1 **Virus**
    - A Computer virus **consists of segments of code that perform malicious** actions.
  - 2.2 **Worms**
    - Is a **malicious program that replicates itself constantly,** until they completely fill available resources, such as memory, harddisk etc.
  - 2.3 **Trojan Horses**
    - Are **software programs that hide their true** nature and reveal their designed behavior only when activated

UNIT -1 Threats

- 2.4 Back Door / Trap Door
  - A virus or worm can have **a payload that installs** a back door component in a system, **which allows the attacker to access the system at will with special privilegs**.
- 2.5 Polymorphic Threats
  - Is one that **over time changes the way it appears** to **antivirus software programs, making it undetectable** by techniques that look for preconfigured signatures.
- 2.6 Worm Hoaxes
  - Well meaning **people can disrupt the harmony** and flow of an organization when they **send group emails warning of supposedly dangerous viruses that dont exist.**

UNIT -1 Threats

3. Deviations in Quality of Service

- IS depends on the successful operation of many interdependent support systems, including power grids, telecom networks, parts suppliers, service vender etc.
- Any of the support systems can be interrupted by storms, employee illnesses or other unforeseen events.
- This degradation of service is a from of **availability Disruption.**
- Internet Service Issue
- Communications and Other Service Provider Issues
- Power Irregularities

UNIT -1 Threats

4. Trespass

- When an **unauthorized individual gains access to the information an organization is trying to protect,** that act is categorized as espionage or trespass.

5. Forces of Nature

- Fire
- Flood
- EarthQuake
- Lightning
- LandSlide / MudSlide
- Tornado
- Hurricane
- Tsunami
- Electrostatic Discharge

UNIT -1 Threats

6. Human Error Or Failure:

- This category includes acts performed without intent or malicious purpose by an authorized user. When people use information systems, mistakes happen. Inexperience, improper training, and the incorrect assumptions are just a few things that can cause these misadventures. Employees are the threat agents closest to the or

UNIT -1 Threats

7. Information Extortion:

- Information extortion occurs when an attacker or trusted insider steals information from a computer system and demands compensation for its return or for an agreement not to disclose it.
- Extortion is common in credit card number theft. For example, Web-based retailer CD Universe was the victim of a theft of data files containing customer credit card information.
- The culprit was a Russian hacker named Maxus, who hacked the online vendor and stole several hundred thousand credit card numbers.
- When the company refused to pay the $100,000 blackmail, he posted the card numbers to a Web site, offering them to the criminal community. His Web site became so popular he had to restrict access.

UNIT -1 Threats

8. Missing, Inadequate or Incomplete Organizational Policy

9. Missing, Inadequate or Incomplete Controls

10. Vandalism

- Category of threat involves the deliberate sabotage of a computer system, **either destory an asset or damage the image of an organization.**

11. Theft

12. Technical Hardware Failures or Errors

13. Technical Sogtware Failures or Errors

14. Technological Obsolescence

- **Outdated infrastructure can lead to unreliable and untrustworthy systems.** There is a risk or loss of data integrity from attacks.

UNIT -1 Attacks

- An Attack is an **act that takes advantage of a vulnerability** to compromise a controlled system.
- The followig are the major types of attacks used against controlled systems.

1) **Malicious Code**

The malicious code attack includes the execution of **Viruses, Worms, Trojan Horses and Active Web Scripts with the intent to destory information.**

- **Bot** (an automated software program that executes certain commands when it receives a specific input)
- **Spyware** (any technology that aid in gathering information about a person or organization without their knowledge)
- **Adware** (any software progrm intended for marketing purposes such as that used to deliver and display advertising banners)

UNIT -1 Attacks

2) **Hoaxes**
   - A more devious attack on computer systems is the **transmission of a virus hoax with a real virus attachment.**

3) **Back Doors**

4) **Password Crack**

   - Attempting to r**everse calculate a password is often called cracking**

5) **Brute Force**

   - The **application of computing and** network resources to **try every possible password combination** is called brute force attack.

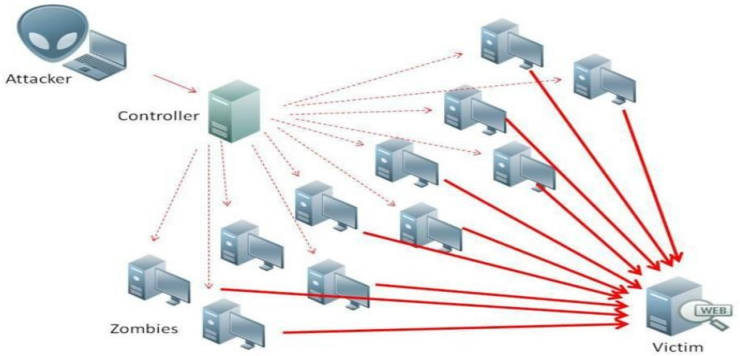
UNIT -1 Attacks

6) Dictionary

- The Dictionary attack is a **variantion of the brute force attack which narrows the field by selecting specific target accounts and using a list of commonly used passwords** instead of random combinations.

7) **Denial-of-Service (DoS) / Distributed Denial–of-Service (DDoS)**

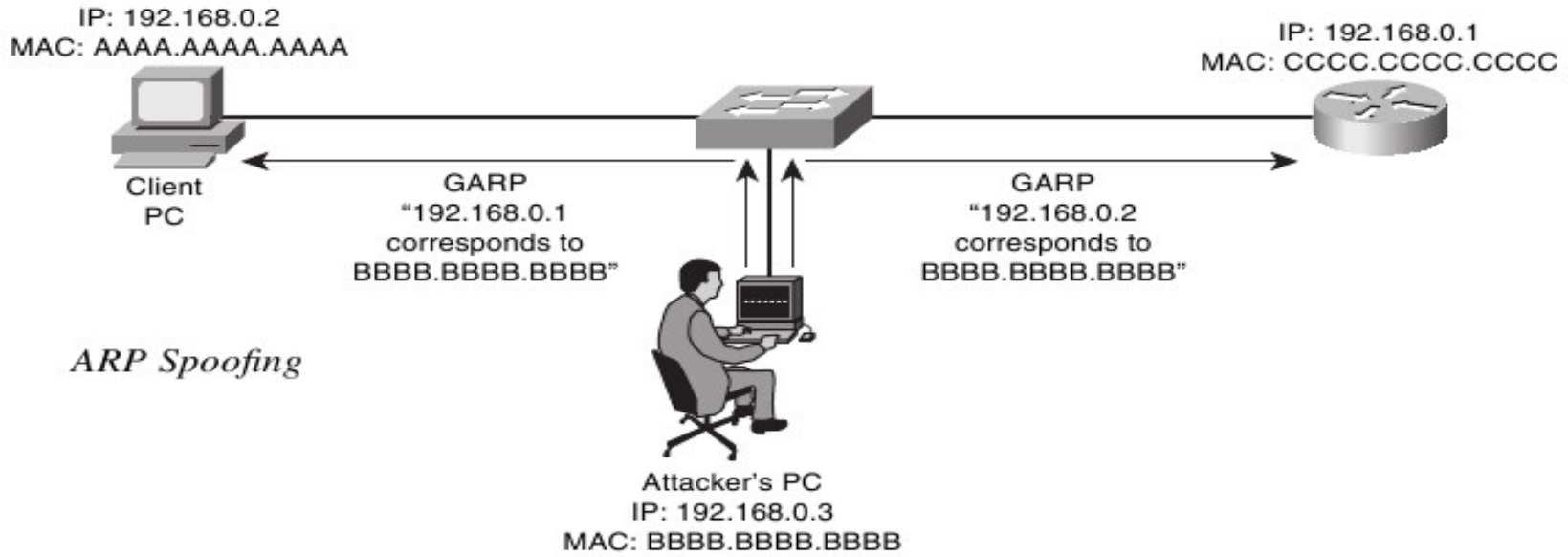
- DoS attack, **the attacker sends a large number of connection or inforamtion requests** to a target, so many requests are made that **the target system becomes overloaded and cannot respond** to requests for service.



UNIT -1 Attacks

8) Spoofing

- Is a **technique used to gain unauthorized access to computers,** wherein the **intruder sends messages with a source IP address** that as been forged to **indicate that the messages are coming from trusted host.**



ARP Spoofing

UNIT -1 Attacks

9) Man-in-the-Middle

- An **attacker monitors packets from the networks, modifies them, and inserts them back** into the network.
- It is also know as **TCP Hijacking attack.**

10) Spam

- Is **unsolicited commercial e-mail, which may consider as trivial nuisance.** It has been used as a means of enhancing malicious code attacks.

11) Mail Bombing

- Other version of Dos is Mail Bombing, **in which an attacker routes large quantities of e-mails to the target**

UNIT -1 Attacks

12) Sniffers

- Is a program or device that can monitor data traveling over a network.
- Sniffers can be used **both for legitimate network management functions and for stealing information.**

13) Social Engineering

- **Is the process of using social skills to convince people to reveal access credentials or other valuable information to the attackers.**

14) Phishing

- Is an **attempt to gain personal or financial information from an individual, usually by posing as a legitimate entity.**

UNIT -1 Attacks

15) Pharming

- Is **“the redirection of legitimate web traffic to an illegitimate site for the purpose of obtaining private information”.**

16)Timing Attack

- A Timing **Attack explores the contents of a web browser's cache and stores a malicious cookie on the client's system.**