

## cyber law & ethics

### Computer Security :-

- Computer security also called cybersecurity is the protection of computer system and information from harm, theft and unauthorised use.
- Computer hardware is typically protected by the same means used to protect their valuable or sensitive equipment - namely, serial numbers, doors and locks and alarm.
- It was used in broad sense to cover the protection of computer & everything associated with it.
- The computer security is the protection of information stored in a computer system.

### Threats to Security :-

#### Types of threats :-

- Natural
- Unintentional
- Intentional.

Natural :- This threats may be every physical plant and piece of equipments  
ex:- fire, floods, power failure

unintentional:- Due to lack of knowledge, ignorance creates dangerous.

Ex:- A user of system administration who was not be trained.

Intensional:-

These are 2 types insides and outsides.

Insides:-

Insides or might be operator of system even a casual user who willing to share a password.

Outsides:-

Outsides may penetrate the system in variety of ways - electronic entry through modem and network connection and bribery of inside personal.

Computer Security mandates and

legislations:-

The Information Technology [The Indian Computer Emergency Response team and manner of performing function and duties].

Rules 2013:

CERT Rules (IT Rules 2013)

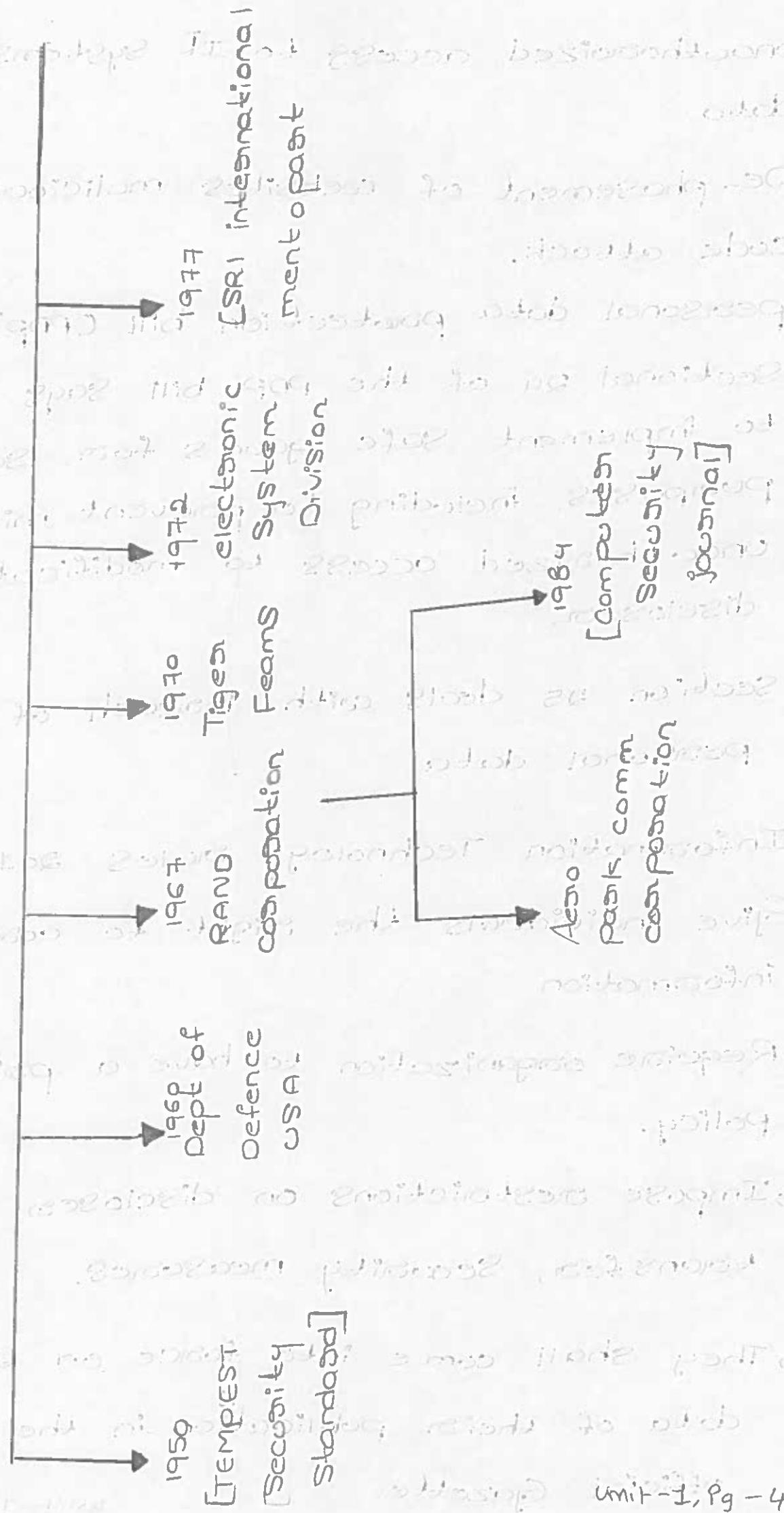
As per the CERT rules

- A targeted intrusion [or] the compromising of critical news on system.
- Unauthorized access to IT Systems [or] data.
- De-phasing of websites malicious code attack.  
Personal data protection bill (PDP) 2019:-
- Sectional 24 of the PDP bill says that to implement safe guards for several purposes, including to prevent misuse unauthorized access to modification disclosure.
- Section 25 deals with breach of personal data.

Information Technology Rules 2011:-

- Give individuals the right to correct information
- Requide organization to have a privacy policy.
- Impose restrictions on disclosure, data transfer, security measures.
- They shall come into force on the data of their publication in the official Gazette.

## Computer security and responses



## Privacy considerations :-

- Privacy means to control that you have over your personal information and how that information is used.
- Personal information is any information that can be used to determine your identity.
- Privacy consideration means way of providing privacy to our personal information.

For example:-

- Instagram, WhatsApp etc.

posting post in Instagram, in that case we may follow some privacy consideration

e.g. - who will see your post.

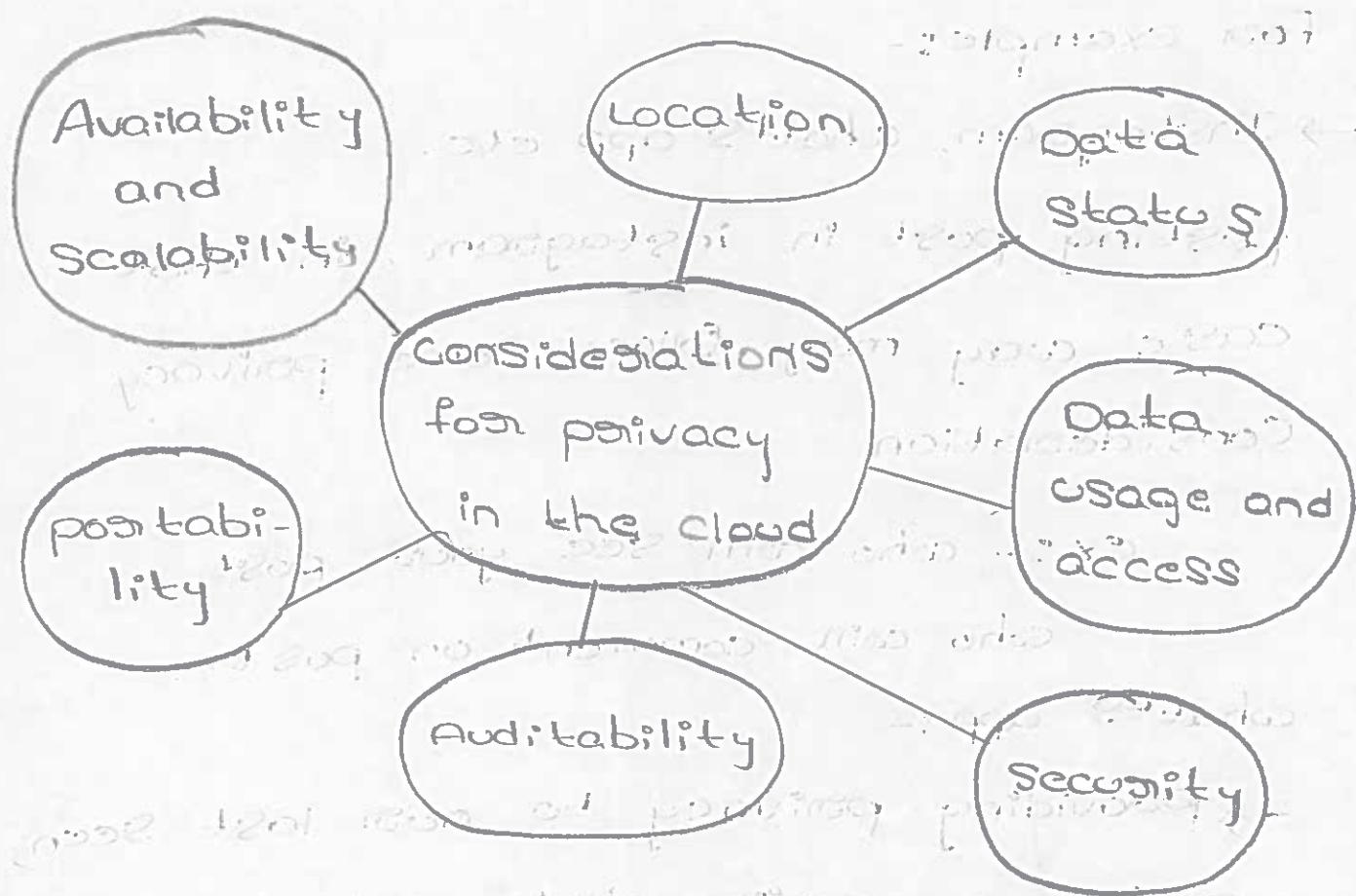
who will comment on post.

WhatsApp:-

- Providing privacy to our last seen, and our profile photo and group setting.

Privacy consideration → Security

- Privacy protection and cyber security should be thought of as interconnected, as more and more personal information is processed or stored online.
- Privacy protection increasingly relies on effective cyber security implementation by organization to secure personal data both when it is in transit and at rest.



## - Information security & its types

### Information protection:-

- Information Security is basically the practice of preventing unauthorized access, use, disclosure, distribution, modification, inspection, recording and destruction of information.
- Information can be physical or electronic one.
- The information Security requirements are Confidentiality, integrity and availability.

### Confidentiality:-

The definition of confidentiality is the state of being secret or of keeping secrets.

### Integrity:-

- It is defined as guarding against improper information modification or destruction.

### Availability:-

- Availability means the information only available to the main users when they need.
- No unauthorised person can access the data.

## Aspects of major elements:-

confidentiality, integrity, availability, authentication and non-repudiation.

## Access control:-

Access control is a data security process that enables organizations to manage who is authorised to access corporate data and resources.

Access control manage through several components.

Identification:- It is a business first means of corroborating that a user who they claim to be.

Ex:- user name.

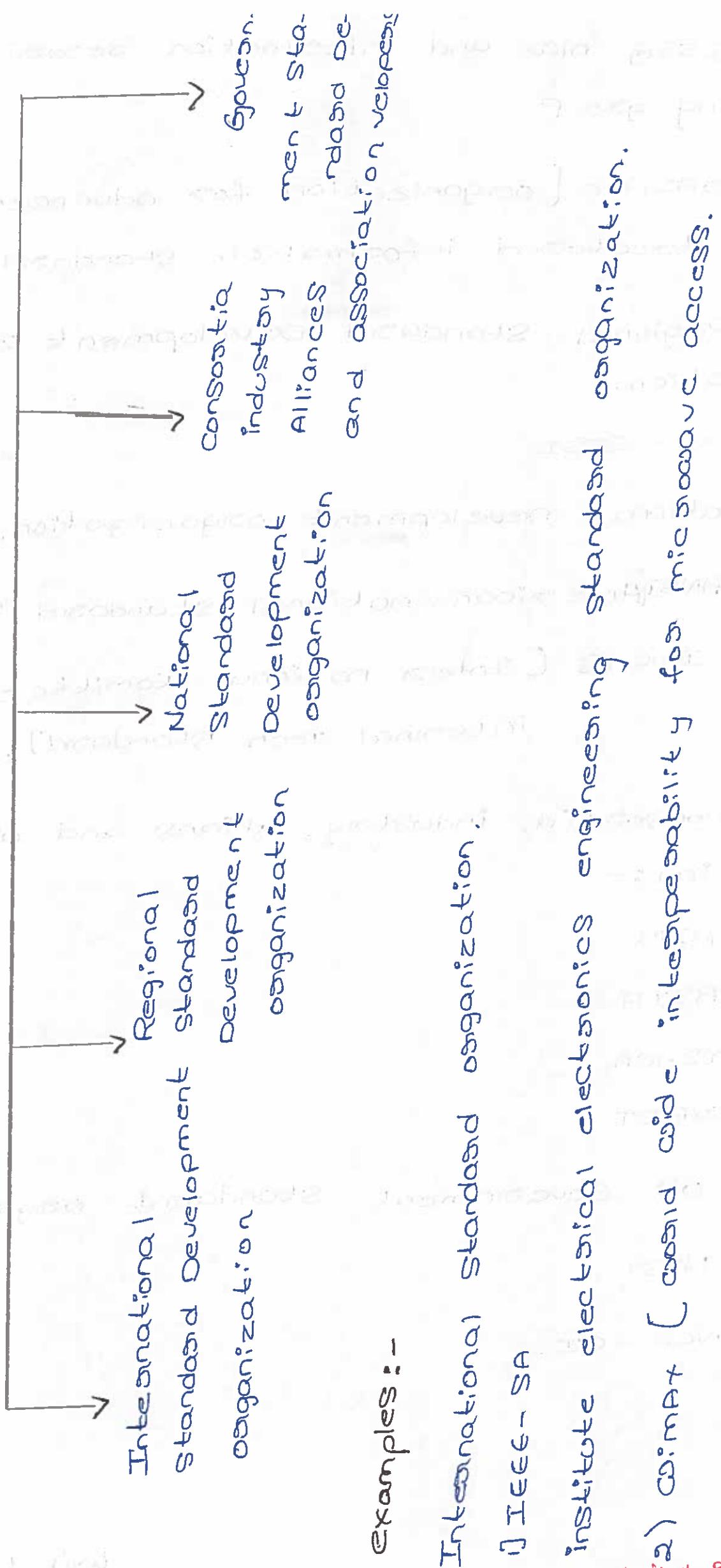
## Authentication:-

It is a cyber security technique used to verify or prove a user's identity. There are main authentication factors:-

- password and pins
- Access cards and keys
- Biometric

4

Cyber security standards developments :-



3] NISSG (new and information Security, steering group).

4] OASIS [organization for advancement of structured information standard.

5] Regional Standard Development organization.

Ex:- EISI

6] National development organization.

→ ANSI [American national standard institute].

→ INCITS [International committee for international Tech Standard].

7] consortia, industry, alliance and association:-

AIM

BSIA

ISACA

COBIT.

8) US Government Standard organization

NIST

NCS - CII.

# Information protection & access control :-

## Access control:-

It regulates the flow of information and detects how a user or a system can connect or interact with other systems or resources.

→ It means of safe guarding your business.

## Identification:-

It is a business first means of corroborating that a user is who they claim to be ex:- user name.

## Authentication:-

It is the cyber security technique used to verify or prove a user's identity. These are main authentication factors

- ① password and pins,
- ② Access & keys,
- ③ Biometrics.

## Biometric:-

Retina

Iris

Finger

Facial Scan.

Voice Scan

## Authorization

Once a person has gone through identification & authentication authorization controls the levels access & ability to change edit or disseminate certain data.

## Counter measures

There are many of counter measures

→ Methods of protecting computers & information.

## Cyber Security :-

It refers to the body of technologies, process and practices designed to protect files, devices programs and data from attack, damage (or) unauthorized access.

## International Security activity :-

International security also called as global security is a term which by states and international organizations, such as the united nations,

European union, and others to ensure mutual survival and safety

## Principles :-

Democracy, governance and rule of law.

Democracy :- For the PPI, off the people by the people.

Governance :- The system by which the rules & regulations followed.

Rule of law :-

We should follow any types of rules.

## Advantages :-

- Benefits of business.
- Common understanding.
- Technical agreements.
- Skills enhancement.
- Efficiency and customer satisfaction.

## Disadvantages :-

Expensive

Lack of knowledge

Not easy to easy

Special experts required.

So to overcome disadvantages we will use some high level technologies

## Computer security :-

Computer security also called cyber security is the protection of computer system and information from harm, theft and unauthorised use.

Computer hardware is typically protected by the same means used to protect their valuable or sensitive equipment - namely, serial numbers, doors and locks and alarm.

It was used in broad sense to cover the protection of computer and everything associated with it.

The computer security is the protection of information stored in a computer.

Personal data protection bill (PDP)  
2019 :-

Sectional 24 of the PDP will says that to implement safe guard for several purposes, including to prevent misuse unauthorized

Access to modification disclosure  
Section 25 deals with breach of  
personal data

Information technology rules 2011 e

Give individuals the right to correct  
information.

Require organizations to have a privacy  
policy.

Impose organization to have a privacy  
policy.

They shall come into force on the  
data of their publication in the  
official Gazette

Privacy considerations

Privacy means to control that you  
have over your personal information,  
and how that information is used

Personal information is any information  
that can be used to determine  
your identity.

→ Privacy protection increasingly relies on effective cyber security for personal data both when it is in transit and at rest

## Orange Book

The orange Book is nickname of the defense Department's Trusted computer system evaluation Criteria, a book published in 1985. The orange book specified criteria for rating the security of different security systems, specifically for use in the government procurement process.

The orange book is used for the publication, Approved Drug - products with Therapeutic Equivalence evaluations (the list, commonly known as the Orange Book), identifies drug products approved on the basis safety and effectiveness by the food and drug administration (FDA) under the federal food, drug and cosmetic Act (the FD&C Act).

These evaluations have been prepared to serve as public information and advice to state health agencies, prescribers, and pharmacists to promote public education in the area of drug product selection and to foster containment of health care costs.

The Orange Book was distributed as a proposal in January 1979. It included only currently marketed prescription drug products approved by FDA through new drug applications (NDAs) and abbreviated new drug applications (ANDAs) under the provisions of section 505 of the FD&C Act and FDA regulations at that time.

The Orange Book is composed of four parts:

- (1) Approved prescription drug products with therapeutic equivalence evaluations.
- (2) approved over-the-counter (OTC) drug products for those drugs that may not be marketed without NDAs or ANDAs because they are not covered under existing OTC monographs.
- (3) drug products with approval under section 505 of the FD&C Act administered by the Center for Biologics evaluation and research.

## Secure System planning and administration

A system security plan is a formal plan that defines the plan of action to secure a computer or information system.

It provides a systematic approach and techniques for protecting a computer from being used by unauthorized users, guards against worms and viruses as well as any other incident/ event process that can jeopardize the underlying system's security.

Typically system security plan includes:

- \* List of authorized personnel /users that can access the system.
- \* Level of access /tiered access, or what each user is allowed and not allowed to do on the system.
- \* Access control methods, or how users will access the system (User ID), password, biometrics.
- \* Strengths and weaknesses of the system and how weaknesses are handled.

\* May also include system backup/ restoration procedures

In the security planning process, the organization identifies which assets require protection and the types of risks that could compromise those assets.

This critical function determines the level of appropriate countermeasure that is required based upon a formally documented process.

Risks are usually categorized into three

Categories:

1. People - human resources are usually the most critical asset within any organization, and as such, must receive a stronger consideration when assessing risk.

2. Property - Physical property or intellectual assets.

3. Legal liability - legal risks can also affect people and property, but need to be considered as a separate category.