MODULE 1 :

INTRODUCTION TO INFORMATION SECURITY

1. Definition Of Information Security:

The state of being protected against the unauthorized use of information.

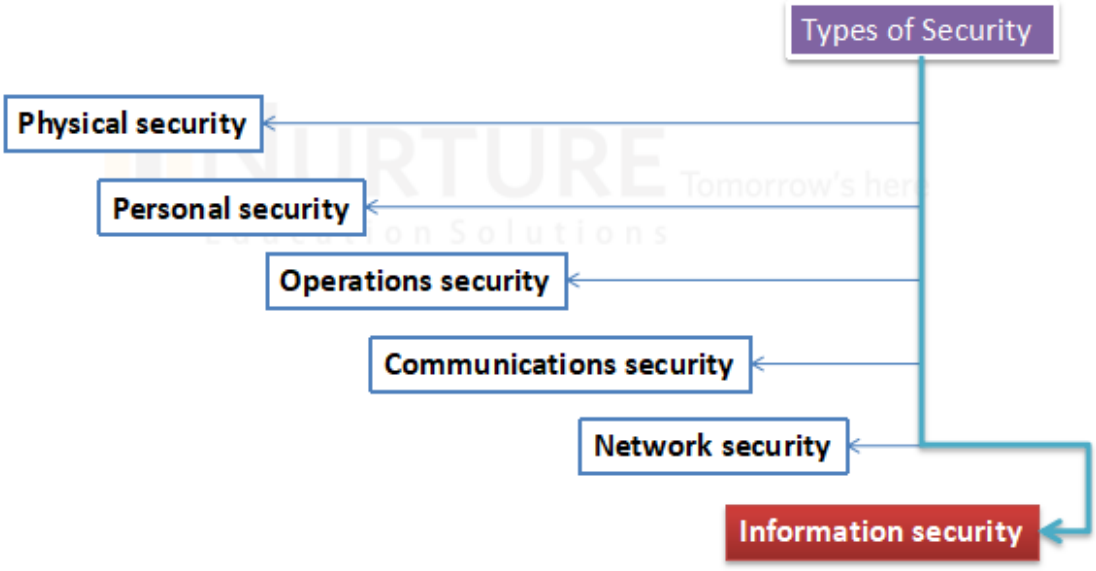
A successful organization should have the following multiple layers of security in place to protect its operations.

Where it has been used?

- ✓ Governments, military, financial institutions, hospitals, and private businesses.
- ✓ Protecting confidential information is a business requirement.

WHAT IS SECURITY?

security is defined as "the quality or state of being secure—to be free from danger."



a. **Physical Security : protection** of personnel, hardware, software, networks and data from **physical** actions and events that could cause serious loss or damage to an enterprise, agency or institution.

b. **Personnel Security :** to protect the individual or group of individuals who are authorized to access the organization and its operations

c. **Operations Security:** to protect the details of a particular operation or series of activities
d. **Communications Security** : to protect communications media, technology, and content
e. **Network Security** : to protect networking components, connections, and contents
f. **Information Security** : to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

2. Evolution (History) of Information Security :

- Computer security began immediately after the first mainframes were developed
- Groups developing code-breaking computations during world war II created the first modern computers
- Physical controls were needed to limit access to authorized personnel to sensitive military locations
- Only rudimentary controls were available to defend against physical theft, espionage, and sabotage
- Department of Defense's Advanced Research Project Agency (ARPA) began examining the feasibility of a redundant networked communications
- Larry Roberts developed the project from its inception

- ARPANET grew in popularity as did its potential for misuse
- Fundamental problems with ARPANET security were identified
  - No safety procedures for dial-up connections to ARPANET
  - Non-existent user identification and authorization to system

- Late 1970s: microprocessor expanded computing capabilities and security threats.
- MULTICS : Much of the early research on computer security centered on a system called Multiplexed Information and Computing Service (MULTICS)
- However it is now obsolete, MULTICS is notable as it was the first operating system to combine security into its core functions.
- It was a mainframe, time-sharing operating system generated in the mid- 1960s by a group of General Electric (GE), Bell Labs and the Massachusetts Institute of Technology (MIT)
- Networks of computers became more common; so too did the need to interconnect networks
- Internet became first manifestation of a global network of networks
- In early Internet deployments, security was treated as a low priority

- The Internet brings millions of computer networks into communication with each other—many of them unsecured
- Ability to secure a computer's data influenced by the security of every computer to which it is connected

3. Basic Principles of Information Security :

The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

Information security includes the broad areas of information security management, computer and data security, and network security.

The CNSS model of information security evolved from a concept developed by the computer security industry called the C.I.A. triangle. The C.I.A. triangle has been the industry standard for computer security since the development of the mainframe.

CIA is called as Security Triad.

It is based on the three characteristics of information that give it value to organizations:

- Confidentiality,
- Integrity, And
- Availability

Confidentiality : Confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Confidentially is a component of privacy that implements to protect our data from unauthorized viewers.

Examples of confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals.

Integrity : Integrity means that data cannot be modified without authorization i.e., maintaining and assuring the accuracy and completeness of data over its entire lifecycle.

Availability: For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning .

Note :

AAA refers to authentication, authorization, and accounting
AAA is used in the process of access control to secured resources

Attributes of Information Security:

a.Confidentiality : Make sure that the necessary level of secrecy is forced at all the junction of data processing and secures unauthorized disclosure. This makes sure that unauthorized users do not interrupt copy or duplicate information.

Threat sources:

- Network monitoring
- Stealing password files

Countermeasures:

- Encrypting data as it is stored and transferred
- Implementing strict access control methods and data classification

b. Integrity : The protection and assurance of the reliability, consistency and accuracy of classified data throughout its life. This means securing concealed and unauthorized changes of data either in storage or whereas it transit

Threat sources:

- Viruses
- Logic bomb

Countermeasures :

- Strict access control
- Intrusion detection

c. Availability : Information should be accessible for use if needed by authorized services and users

Threat sources

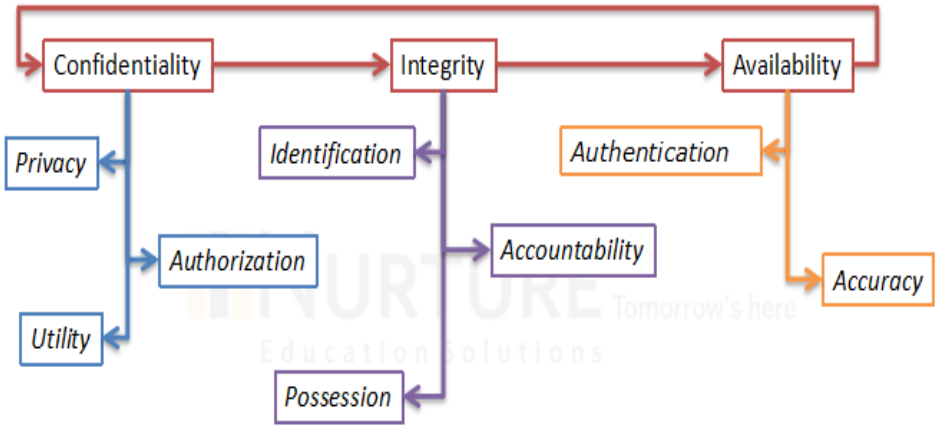
- Device or software failure
- Denial-of-service (DoS) attacks

Countermeasures

- Preserving backups to restore the failed system
- IDS to check the network traffic and host system activities

4. Critical concepts of Information Security:

- The value of information comes from the concepts it possesses
- When a concept of information changes, the value of that information either increases or more commonly decreases
- Some concepts affect information's value to users more than others do, this can depend on circumstances
- Example, timeliness of information can be a critical factor, because information loses much or all of its value when it is delivered too late



Critical Characteristics Of Information :

The value of information comes from the characteristics it possesses.

Privacy	Accountability
Identification	Accuracy
Authentication	Utility
Authorization	Possession

- **Privacy** – Legal Use - It related to individual person E.g. Keeping credit card information by bank is 'Privacy'
- **Identification** – It is ability to identify uniquely a user of a system or an application. Ex. Who you claim to be? Username , Bio metrics…

- **Authentication-** which we use to describe situations when we need to identify who we are and we prove that we are who we say we are ,
  - ✓ Something a person or entity knows- Password
  - ✓ Something a person or entity has – ID cards
  - ✓ Something a person is – retina, finger prints
  - ✓ For example, username and password is one mode of authentication
- **Authorization**- which we use to describe what access authenticated user has. Basically, we describe what the user is authorized to work with.
  - ✓ Authorization for each user
  - ✓ Authorization for member group
- **Accounting**- which is used to describe logging. Logging means keeping track of what someone did on the system
- **Accuracy** – Free from Mistakes or Error
- **Utility** - Utility of information is the quality or state of having value for some purpose or end. Information has value when it can serve a purpose
- **Possession** - Possession of information is the quality or state of ownership or control
  Information is said to be in one's possession if one obtains it, independent of format or other characteristics

Some other Concepts:

a. **Access :** the ability to use, alter or refer an information sytem.Authorised user will have legal access to information whereas hackers will have illegal access.

b. **Accountability :** ensures that all the actions on a system such as authorised or unauthorised can be attributed to an authenticated identity.

c. Asset : An asset can be logical (website inf/data) or physical (computer system, person or the real world object). Information security efforts are attempting to protect asset.

d. Attack : An **attack** is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission.

e. Cipher : it is an encrypted text / A **cipher** is a method of hiding words or text with encryption by replacing original letters with other letters, numbers and symbols through substitution or transposition.

f. Cryptoraphy : is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

g. **Electronic Signature :** it is a process that operates on a message to ensure message aunthentication,integrity and source non-repudiation.

h. Encryption : is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot

i. Exploit : A technique used to compromise a system.

j. Exposure : A condition or state of being exposed.

k. Loss : instance of information damage or unauthorised modification. When an organisation's information is stolen- considered as a loss.

l. Non-Repudiation : is a method in which the data sender is provided with proof of delivery and the receiver confirms the seder's identity. This concept is associated with 'electronic signature'.

m. Policy : is a general commitment or direction which decribes what is allowed and not allowed in an organisation.

n. Procedure : A series of actions/steps followed to perform a specific task.

o. Risk : The possibility that something wrong or unwanted will happen . organisations must minimise the risk to protect the information.

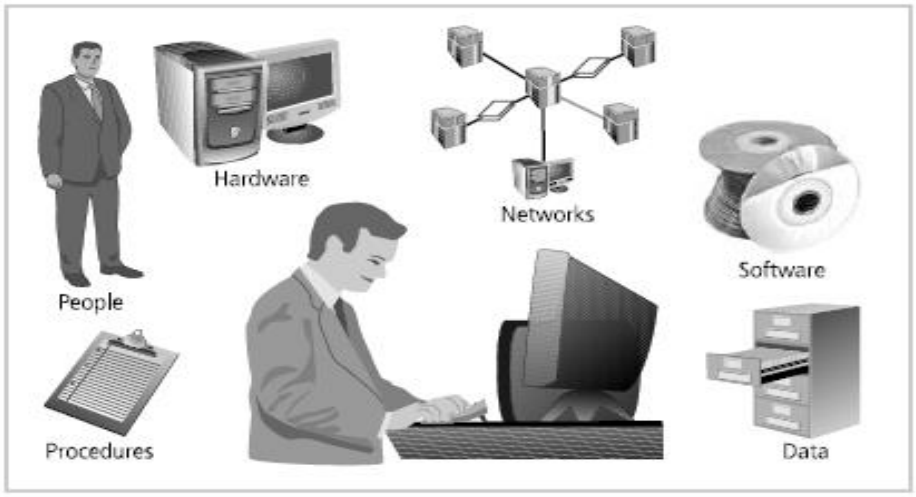
p. Standards : A **standard** is a level of quality or achievement or a document, especially a level that is thought to be acceptable(formally authorised). A**standard** is something that you use in order to judge the quality of something else

q. Threats : Threat is an event that can cause serious harm to a computer system / information. A **threat** is something that may or may not happen, but has the potential to cause serious damage.

r. Vulnerability : the quality or state of being exposed to the possibility of being attacked or harmed.

5. Components of information System

- ✓ Information system (IS) is much more than computer hardware
- ✓ It is the whole set of software, hardware, data, people, procedures and networks which make probable the use of information resources in the organization
- ✓ These six critical components enable information to be input, processed, output and stored
- ✓ Each of these IS components has its own strengths and weaknesses and also as its own characteristics and uses and also has its own security needs.



a. **Software :** The software components of IS comprises applications, operating systems, and assorted command utilities. Software programs are the vessels that carry the lifeblood of information through an organization.

b. **Hardware :** Hardware is the physical technology that houses and executes the software, stores and carries the data, and provides interfaces for the entry and removal of information from the system

c. **Data :** Data stored, processed, and transmitted through a computer system must be protected

d. **People :** There are many roles for people in information systems. Common ones include :
   - ✓ Systems Analyst
   - ✓ Programmer
   - ✓ Technician

e. **Procedure :** A procedure is a series of documented actions taken to achieve something. A procedure is more than a single simple task.

f. Networks : When information systems are connected to each other to form Local Area Network (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge.

❖ Securing Components

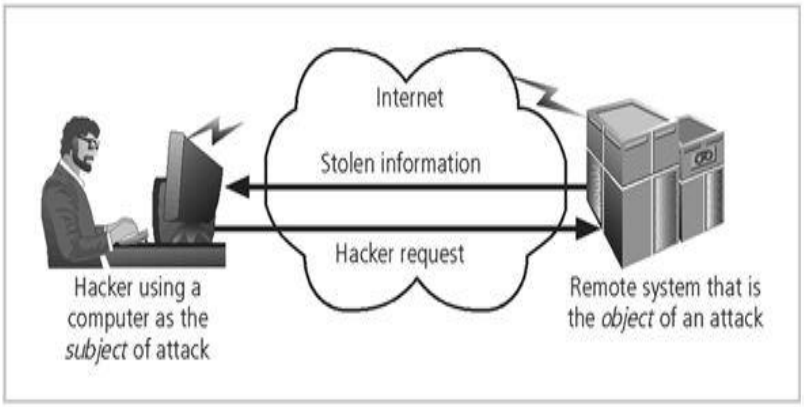
The computer can be either or both the subject of an attack and/or the object of an attack.

- ✓ **Subject of an attack** – Computer is used as an active tool to conduct the attack.
- ✓ **Object of an attack** – Computer itself is the entity being attacked

Two types of attacks

Direct attack: When a Hacker uses his personal computer to break into a system.

Indirect attack : A system is compromised and used to attack other system



6. Balancing Information Security & Access

- ✓ Information security should balance protection and availability
- ✓ It is possible to make a system available to anyone, anywhere, anytime, through any means
- ✓ However, such unrestricted access poses a danger to the integrity of the information

- ✓ On the other hand, a completely secure information system would not allow anyone access
- ✓ To achieve balance—that is, to operate an information system that satisfies the user and the security professional
- ✓ Level of security must allow reasonable access, yet protect against threats
- ✓ An imbalance can occur when the needs of the end user are undermined by heavy a focus on protecting and administering the information systems
- ✓ Both information security technologists and end users- recognize that both groups share the same overall goals of the organization
- ✓ To ensure the data is available when, where, and how it is needed, with minimal delays or obstacles
- ✓ In an ideal world, this level of availability can be met even after concerns about loss, damage, interception, or destruction have been addressed

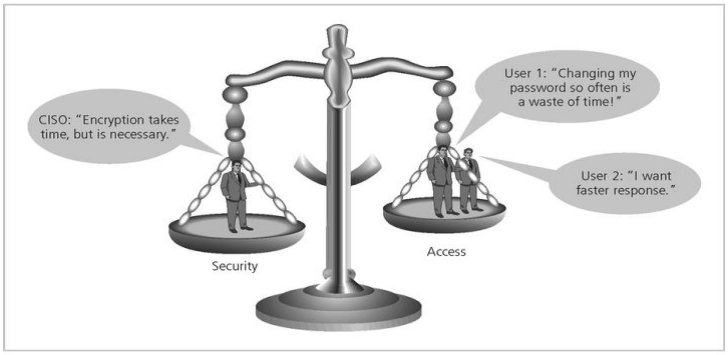


FIGURE 1-6 Balancing Security and Access

Balancing of information security and access can be achieved by following three important principles of information security.

1. **Need to know**
2. **Least privilege**
3. **Separation of duties.**

a. Principles of Least privilege

- The principle of least privilege is the practice of limiting access to the minimal level that will allow normal functioning
- Applied to employees, the principle of least privilege translates to giving people the lowest level of user rights that they can have and still do their jobs

- Example

  - ✓ A backup user does not need to install software
  - ✓ Hence, the backup user has rights only to run backup and backup-related applications
  - ✓ Any other privileges, such as installing new software, are blocked.

- Benefits of the principle include
  1. Better system stability
  2. Better system security 3. Ease of deployment

b. Need to know

- This is an extension of least privilege principe.
- a/c need to know principle , if a user does not need access to a resource to perform a task then the user should not have the right to access that resource.
- Need-to-know also aims to discourage "browsing" of sensitive material by limiting access to the smallest possible number of people.
- Example : in the security clearance system of the U.S government just because a user has clearance to see any secret document, he cannot demand to see any secret document. Instead users are allowed to access documents that are relevant to the task they are supposed to perform.
- To implement this principle, organisations use **'information classification policy'-** determine who should have access to it.
- Example :

- ✓ All employees 'need-to-know' a company's leave policy but not the public, hence it is classified as '**Confidential'.**
- ✓ Information disclosed in website classified as '**public'.**
- ✓ All employees need to know the financial reports of a company; hence it is classified as a **'highly confidential'.**
- ✓ Sensitive government information related to a country's defence is classified as **'secret'.**

c. Separation of Duties

- Refers to segregating the roles & responsibilities of various individuals, so that no single person can subvert a critical process step.
- Ensures that no single person is authorised to perform all activities or steps in a particular process.
- Example : in a financial system to issue cheques, there will be two persons, one to initiate the request for a payment and another to authorise the same payment. In purchase an employee who raises the request cannot approve it and an employee who is authorised to approve a purchase request cannot raise a request.

7. Implementing IT security

- Implementing information security involves identifying specific threats and creating specific controls to counter those threats
- The essential elements of an effective IT security program

  - Periodically assess risk
  - Document an entity-wide security program plan
  - Establish a security management structure and clearly assign security responsibilities
  - Implement effective security-related personnel policies
  - Monitor the security program's effectiveness and make changes as necessary.
  -

❖ Approaches to Information Security Implementation

- Its an incremental process requires coordination, time and patience.
- Two type of approaches

  - ✓ Bottom Up Approach
  - ✓ Top Down Approach

▪ Bottom Up Approach

- ✓ Security may start from the bottom level in which system administrators try to improve the security of their systems.
- ✓ This is referred to as bottom up approach.
- ✓ The operational staff initiate the process and then transmit their findings to the top levels.
- ✓ Advantage : technical expertise of the individual administrators- they work with information systems on a day to day basis and thus acquire in depth knowledge, which is used to enhance the development of an information security system.
- ✓ But this approach doesnot work in all conditions due to the lack of practical support.

▪ Top-down approach :

- ✓ Security is initiated by upper level managers.
- ✓ They issue policies, proceduresand process, prescribe the goals and expected outcome and determine the accountability for each required action.
- ✓ So there exists a higher probability of success.
- ✓ This approach has upper managementsupport, dedicated funding, clear planning and implementation process and the means of influencing organisational culture.

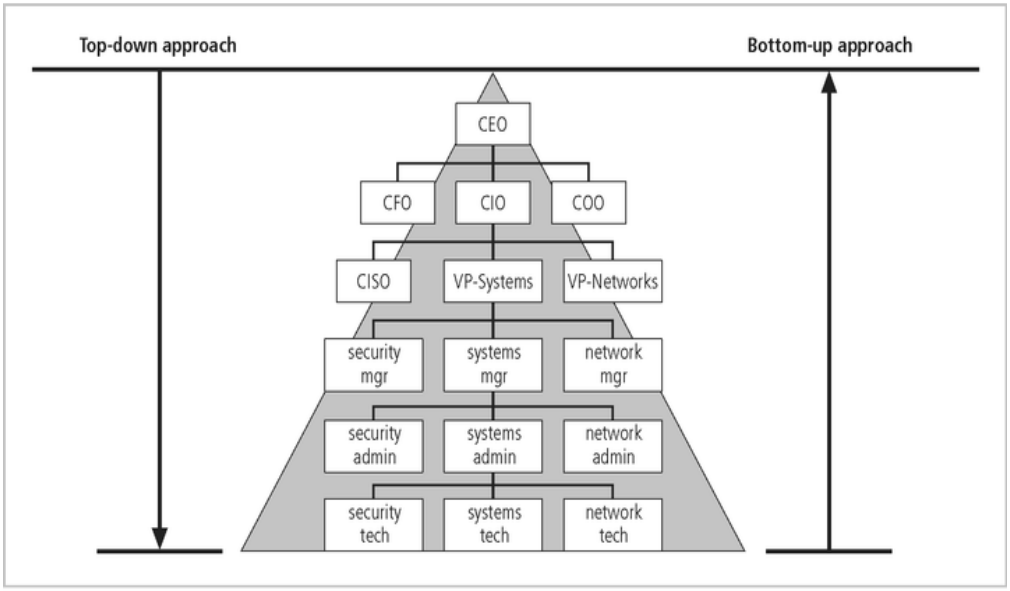


FIGURE 1-7 Approaches to Security Implementation

8. The System Development Life Cycle :

- SDLC is a detailed plan to create, develop, test and eventually implement a software
- Software development is a complex process and to manage this complexity of number of SDLC models or methodologies have been created.
- This process includes different phases such as initiation, analysis, design, implementation, maintenance and disposal.

Benefits of integrating security into SDLC:

1. Premature identification and mitigation of security vulnerabilities.
2. Awareness of possible engineering challenges caused by mandatory security.
3. Identification of shared security services and reuse of strategies and tools.
4. Improved integration and interoperability.
5. Important security decisions are documented during development phase to ensure the security considerations.

Phases of SDLC :

1. Initiation Phase :

- First phase of SDLC.
- During this phase, the organisation establishes system requirements for documentation purpose.
- Security planning should begin with this phase with the identification of key security roles & also information security officer should be identified.

2. Development Phase :

- This phase begins with the information collected during initiation phase.
- During this phase the system is designed, programmed, or developed.
- Main security activity in this phase is conducting risk assessment and these results are used to implement security controls.

3. Implementation Phase :

- In this phase the organisation configures & enables system security features.
- These features are tested for their functionality and installed or implemented on the system by obtaining a formal authorisation to operate the system.
- Before placing the system into operation, design reviews and system tests should be performed to make sure that it meets all the requirements of security specifications.
- The same thing will be documented and maintained as official records in an organisation.

4. Operation and Maintainance Phase :

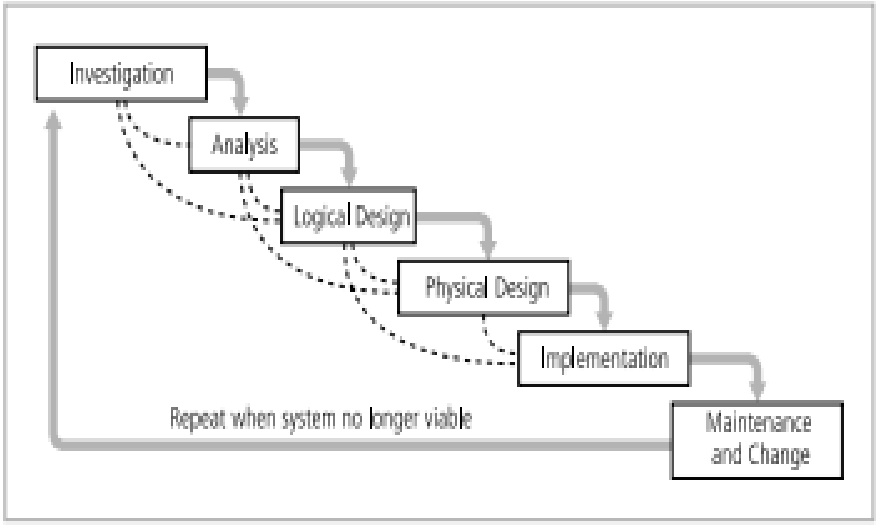
- In this phase the systems and products are in place and enhancement or modification in this system is developed.
- Hardware & software components may be added or replaced.

5. Disposal (Sunset) :

- In this phase plans are developed for discarding system information, hardware, software and to form the transition to a new system.

Security System Development Life Cycle:

- This is same as SDLC, it differs from SDLC by identifying threats and creating specific controls to those threats.



- Phases :

i. Investigation :

- This is the first phase of SecSDLC
- Begins from the upper management.
- Upper management defines process, goals,project and outcomes, budget and other constraints.
- A group of authorised managers, employees and clients are formed to analyse the problems,scope & objective of the project.
- These groups are responsible to check whether the goals & objectives of the project are covered or not in the program policy and are defined.

ii. Analysis :

- In this phase documents are examined and are studied.
- The development team initially examines the existing security policies or programs and documented existing threats and controls associated with it.
- Analyse the related legal issues, which may affect the design of the security solutions.

iii. Logical design :

- Here the rough model of information security is created and developed.
- It examines and implements the key policies that influence the decisions.
- It also addresses the incident response and actions that have to be taken care of during partial or catstrophic loss or damage.
    - Disaster recovery : what must be done to recover information and system immediately after a disastrous event?
    - Incident response : what steps are taken when an attack occurs?
    - Continuity planning : how will business continue in the event of a loss?

iv. Physical Design:

- Evaluates the information security technologies needed to support the blueprint outlined in the logical design and determines a final design.
- Blueprint might be revisited to keep in accordance with changes needed when the physical design is completed.
- T the end of this stage, a feasibility study determines the readiness of the organisation for the proposed project & then it is presented to professionals.

v. Implementation :

- This phase is same as implementation phase in SDLC
- Security solutions are tested and implemented & this process is repeated several times.
- Minor problems & issues are evaluated and specific training education programs are conducted.
- Finally, the tested package is presented to senior management for final approval.

vi. Maintenance & change :

- This is the last & an important phase of SecSDLC.
- Requires constant monitoring, testing, updating & repairing.

9. Security Professionals & the Organisation

The following describes the information security responsibilities of various professionals in an organisation:

I. Senior Management

a) **Chief Information Officer (CIO)**

- ✓ Senior technology officer
- ✓ Primarily responsible for advising senior executives on strategic planning

b) **Chief Information Security Officer (CISO)**

- ✓ Primarily responsible for assessment, management, and implementation of IS in the organization
- ✓ Usually reports directly to the CIO

II. Information Security Project Team

A number of individuals who are experienced in one or multiple requirements of both the technical and non-technical areas:

- The champion : Senior Executive ,promotes project and ensures support both financially and administratively
- The team leader : Project Manager ,who understand Project Management and info security technical requirements.
- Security policy developers: individuals who understands organizational culture ,policies and requirements for successful implementation.
- Risk assessment specialists: individuals who understands financial risk assessment techniques.
- Security professionals : Dedicated , trained and well educated specialists both technically and non technically.
- Systems administrators : Individuals with the primary responsibility for administering the systems .
- End users : Those whom the new system will most directly affect.

III. Data Responsibilities :

- **Data Owner** - responsible for the security and use of a particular set of information. Member of senior management.
- **Data Custodian** – working directly with data owners, responsible for the storage, maintenance, and protection of the information .
- **Data Users** - the end systems users who work with the information to perform their daily jobs supporting the mission of the organization