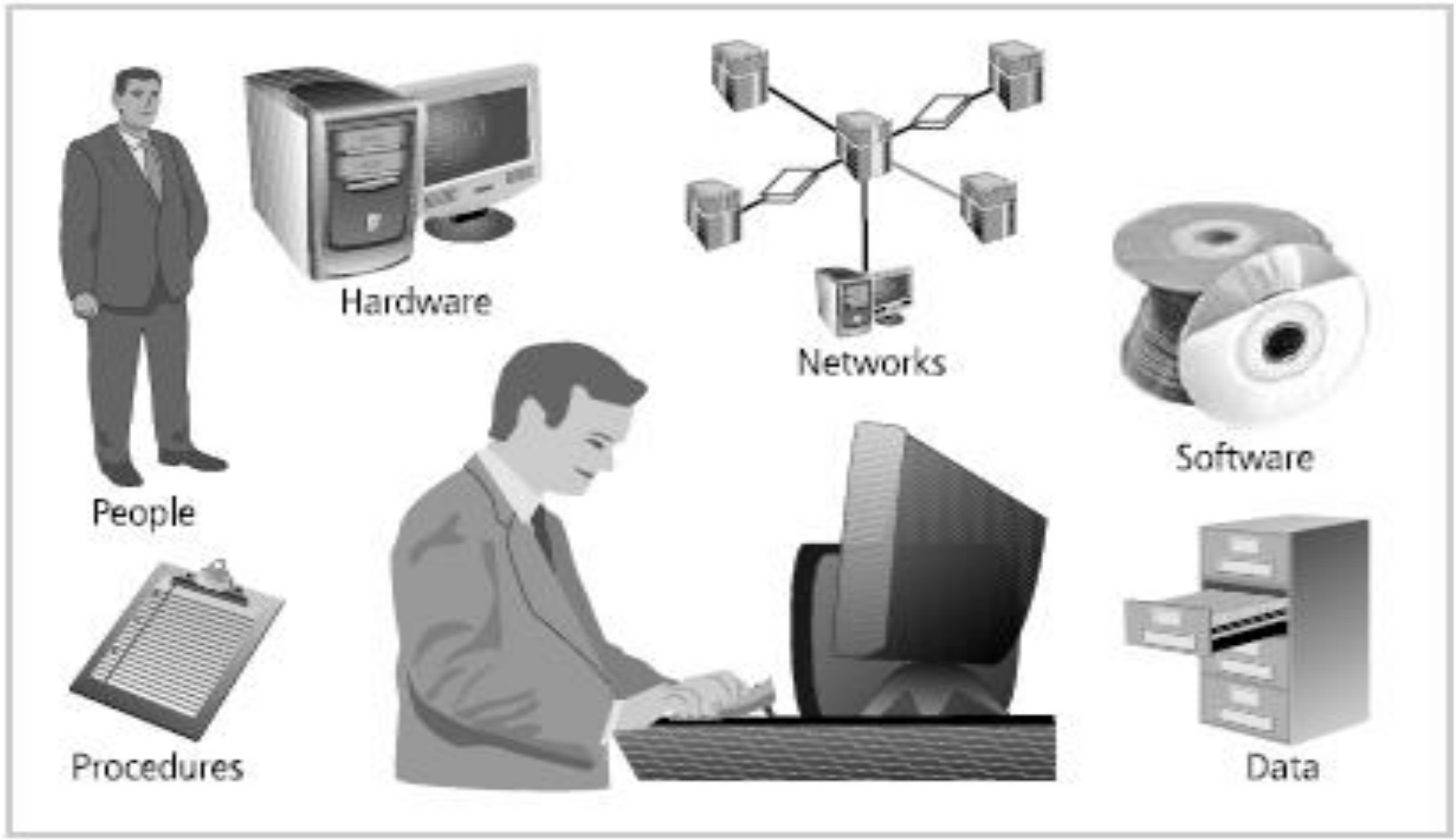
UNIT I

Introduction to Information System Security

Components of Information System

- It is the entire set of software, hardware, data, people, procedures, and networks that make possible 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, as well as its own characteristics and uses.
- Each component of the information system also has its own security requirements.

Components of Information System



Components of Information System

- Software
- Hardware
- Data
- People
- Procedures
- Networks

Components of Information System

- Software
  - The software component of the IS comprises applications, operating systems, and assorted command utilities.
  - most difficult IS component 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.
  - In fact, many facets of daily life are affected by buggy software, from smartphones that crash to flawed automotive control computers that lead to recalls.
  - Software carries the lifeblood of information through an organization. Unfortunately, software programs are often created under the constraints of project management, which limit time, cost, and manpower.
  - software programs become an easy target of accidental or intentional attacks.

Components of Information System

- Hardware
  - Hardware is the 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 from harm or theft.
  - Applying the traditional tools of physical security, such as locks and keys, restricts access to and interaction with the hardware components of an information system.
  - Securing the physical location of computers and the computers themselves is important because a 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.

Components of Information System

- Data
  - Data stored, 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 management systems.
  - 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.

Components of Information System

- 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 commonplace nature of human error.
  - It can be used to manipulate the actions of people to obtain access information about a system

Components of Information System

- Procedures
  - 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
  - Most organizations distribute procedures to their legitimate employees so they can access the information system, but many of these companies often fail to provide proper education on the protection of the procedures.
  - Educating employees about safeguarding procedures is as important as physically securing the information system.
  - After all, procedures are information in their own right. Therefore, knowledge of procedures, as with all critical information, should be disseminated among members of the organization only on a need-to-know basis.

Components of Information System

- Network
  - 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.
  - Steps to provide network security are essential, as is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises

Components of Information System

References

1. Michael E. Whitman, Herbert J Mattord, Principles of Information Security, Sixth edition, Vikas Publishing House, 2017

Thank You