IT 308

INFORMATION ASSURANCE & SECURITY

Pagsibigan, Arvin V.
Antonio, Lilibeth G.
Mangahas, Teresita
Crisostomo, Ma.Ruby Angela J.

LESSON

01

INTRODUCTION TO INFORMATION SECURITY

This lesson will cover essential topics about Information Security.

The lessons under this unit includes the History of Information Security(IS), Key Terms and Definitions, Components of IS, Approaches of IS Implementation.

LEARNING OBJECTIVES

At the end of this lesson, you should be able to:

01 Understand the definition of information security

02 Comprehend the history of computer security and how it evolved into information security

03 Define key terms and critical concepts of information security

04 Enumerate the phases of the security systems development life cycle

05 Define the information security roles of professionals within an organization.

DURATION: 3hrs

INTRODUCTION

Information security: a “well-informed sense of assurance that the information risks and controls are in balance.” —James Anderson, Inovant (2002)

The U.S. Government’s National Information Assurance Glossary defines INFOSEC as: “Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.”

THE HISTORY OF INFORMATION SECURITY

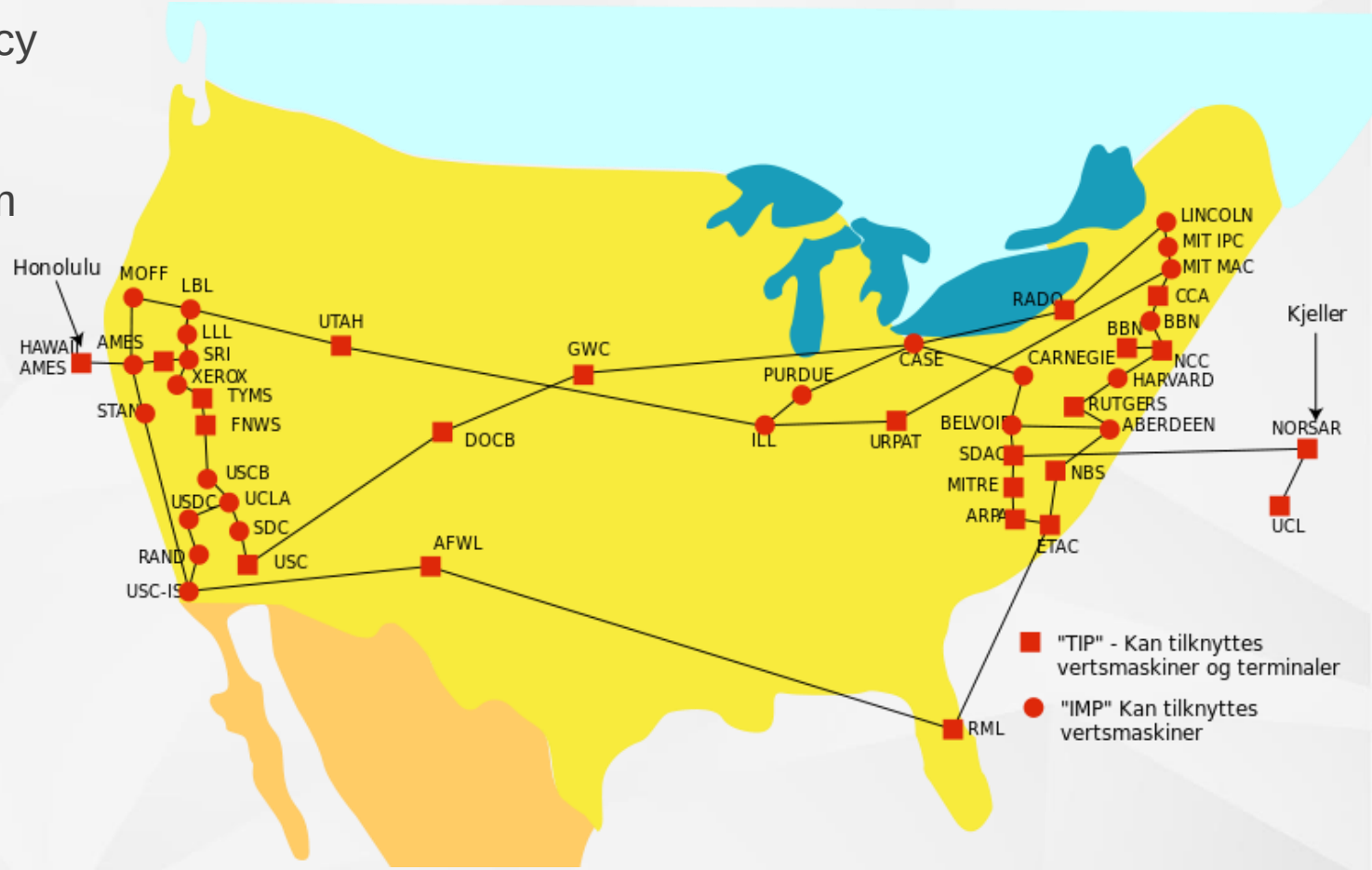
- Began immediately after the first mainframes were developed
- Groups developing code-breaking computations during World War II created the first modern computers
- Physical controls to limit access to sensitive military locations to authorized personnel
- Rudimentary in defending against physical theft, espionage, and sabotage

The Enigma Machine

Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or Unterseeboot version of the Enigma, caused considerable anguish to Allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. ”Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn’t read it.”

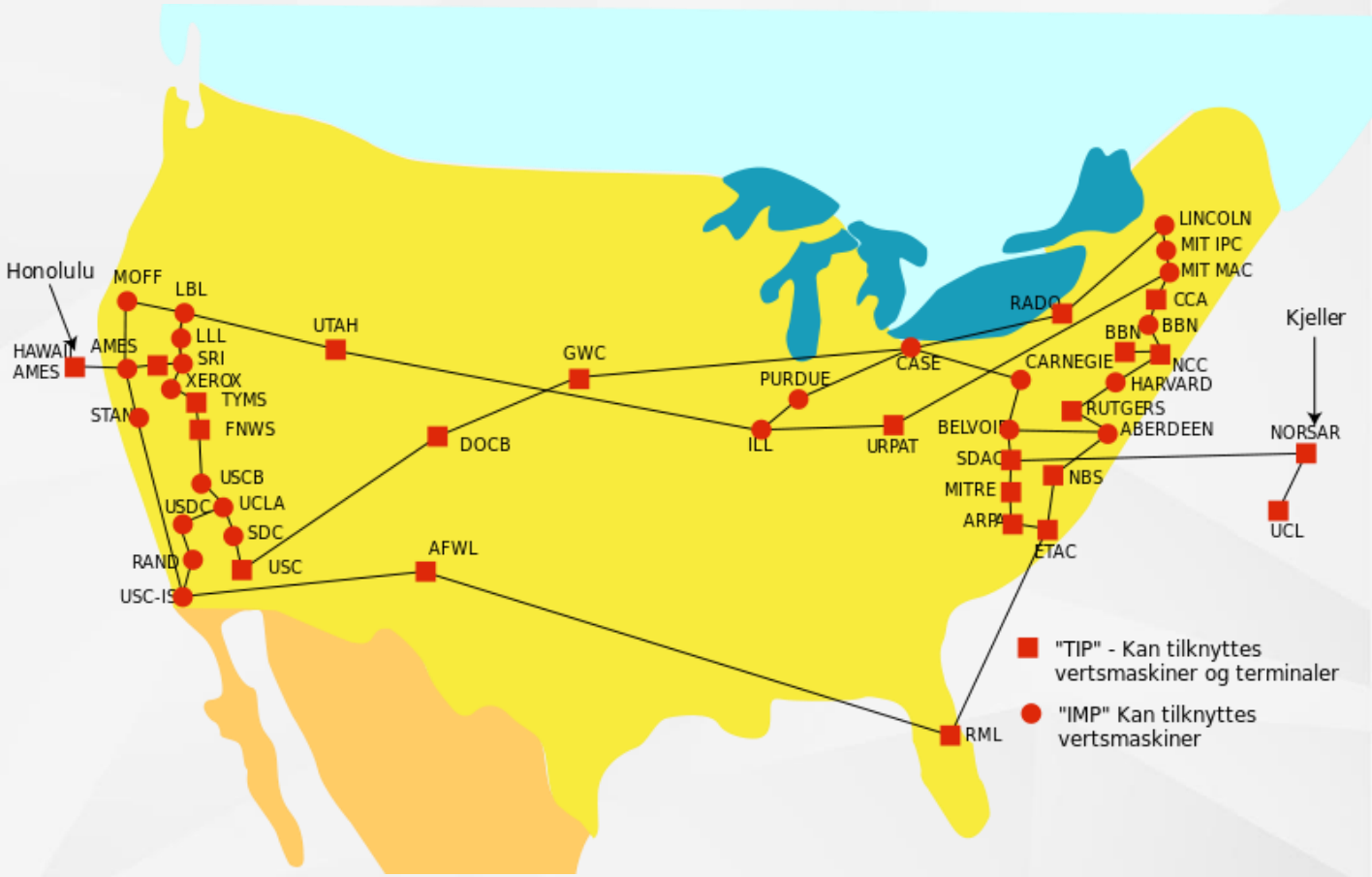
THE 1960'S

- Advanced Research Procurement Agency (ARPA) began to examine feasibility of redundant networked communications
- Larry Roberts developed ARPANET from its inception



THE 1970'S AND 80'S

- 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



R-609

- Information security began with Rand Report R-609 (paper that started the study of computer security)
- Scope of computer security grew from physical security to include:
- Safety of data
- Limiting unauthorized access to data
- Involvement of personnel from multiple levels of an organization

Rand Report R-609- Network Vulnerabilities

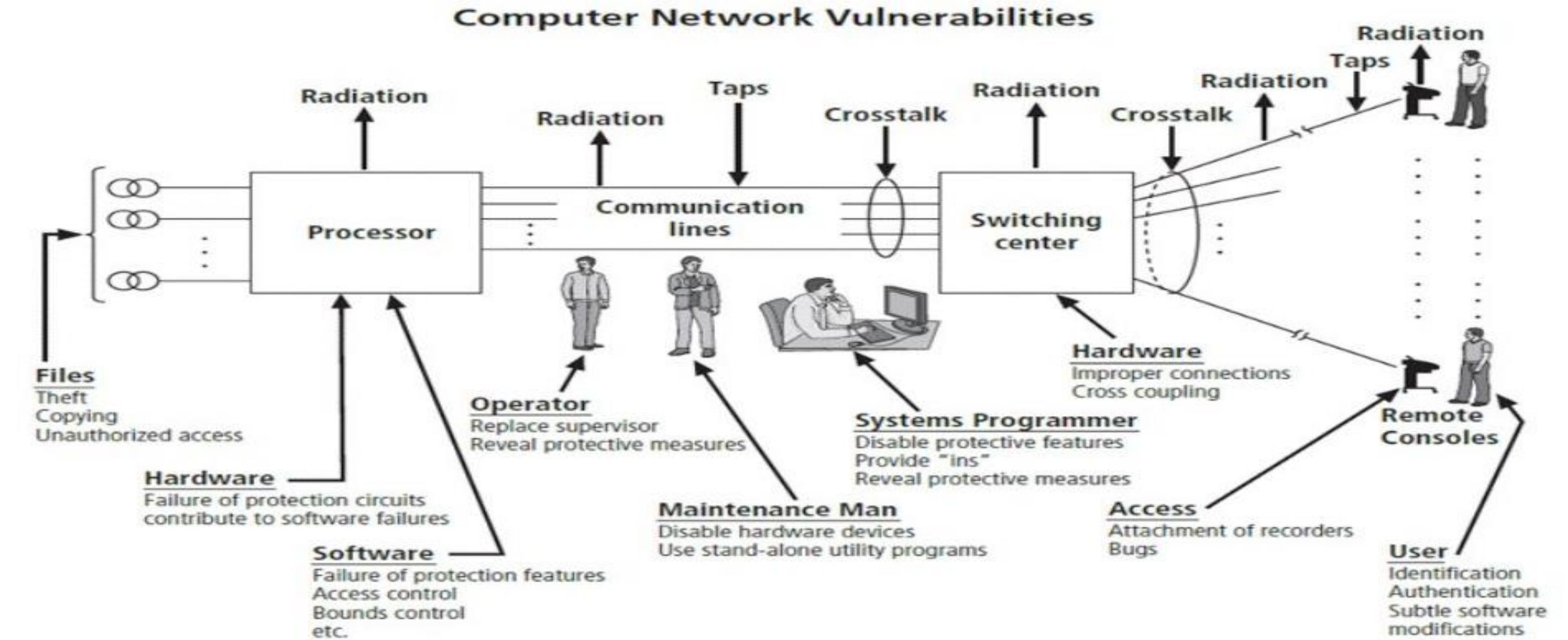


Figure 1-4 Illustration of computer network vulnerabilities from Rand Report R-609

THE 1990'2

- 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

2000 TO THE PRESENT

- 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

WHAT IS SECURITY?

- “The quality or state of being secure—to be free from danger”
- A successful organization should have multiple layers of security in place:
- Physical security
- Personal security
- Operations security
- Communications security
- Network security
- Information security

WHAT IS INFORMATION SECURITY?

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle was standard based on confidentiality, integrity, and availability
- C.I.A. triangle now expanded into list of critical characteristics of information

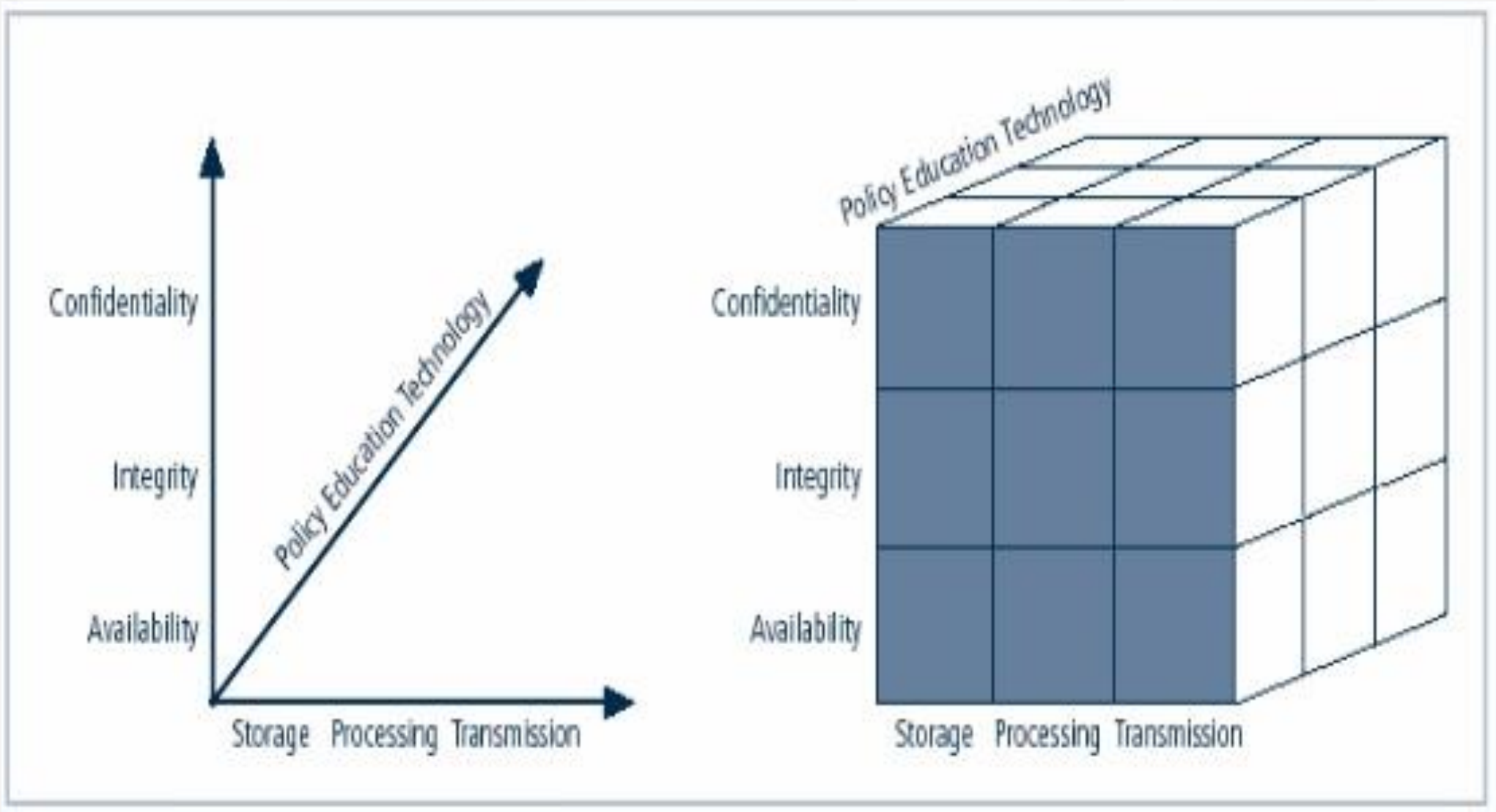
CIA TRIANGLE

CRITICAL CHARACTERISTICS OF INFORMATION

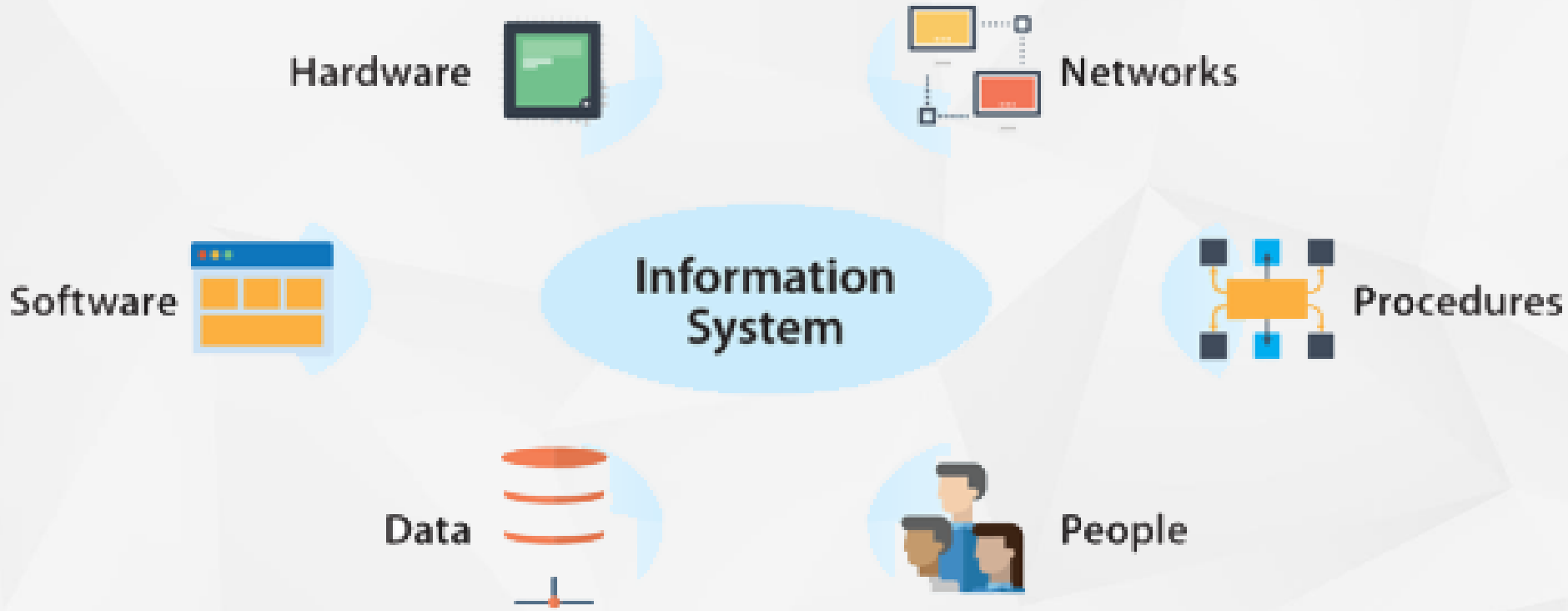
The value of information comes from the characteristics it possesses:

- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity
- Utility
- Possession

CNSS SECURITY MODEL

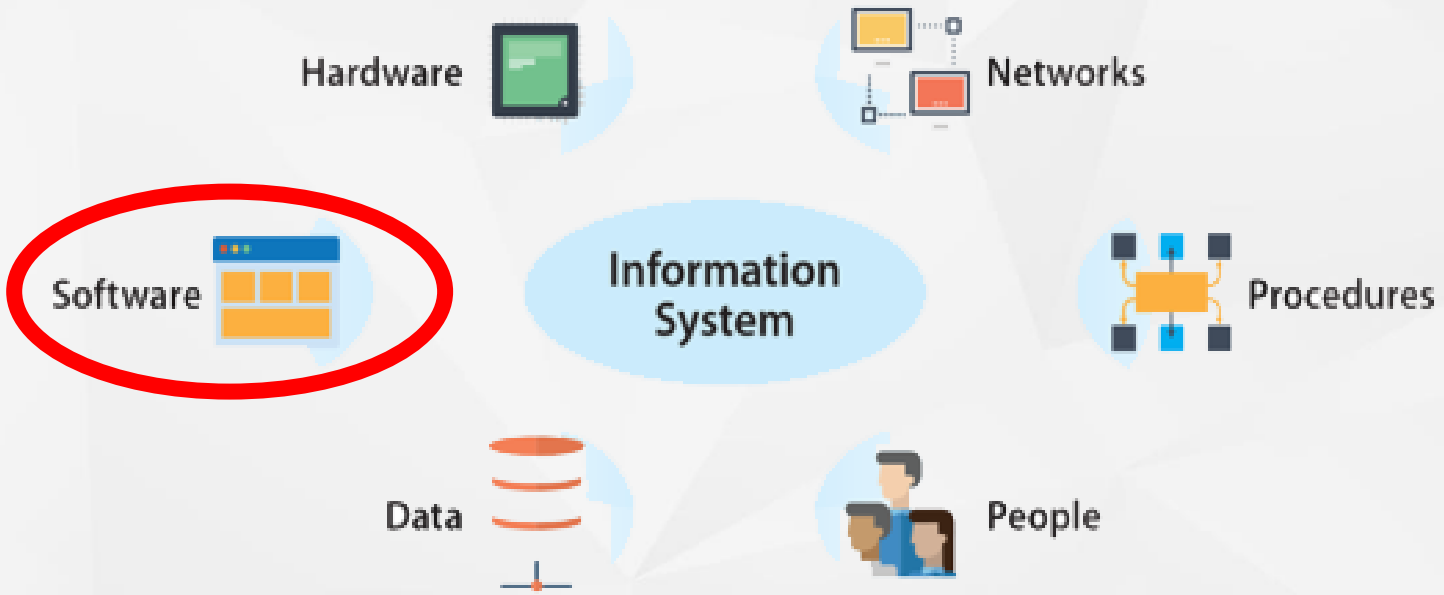


COMPONENTS OF AN INFORMATION SYSTEM



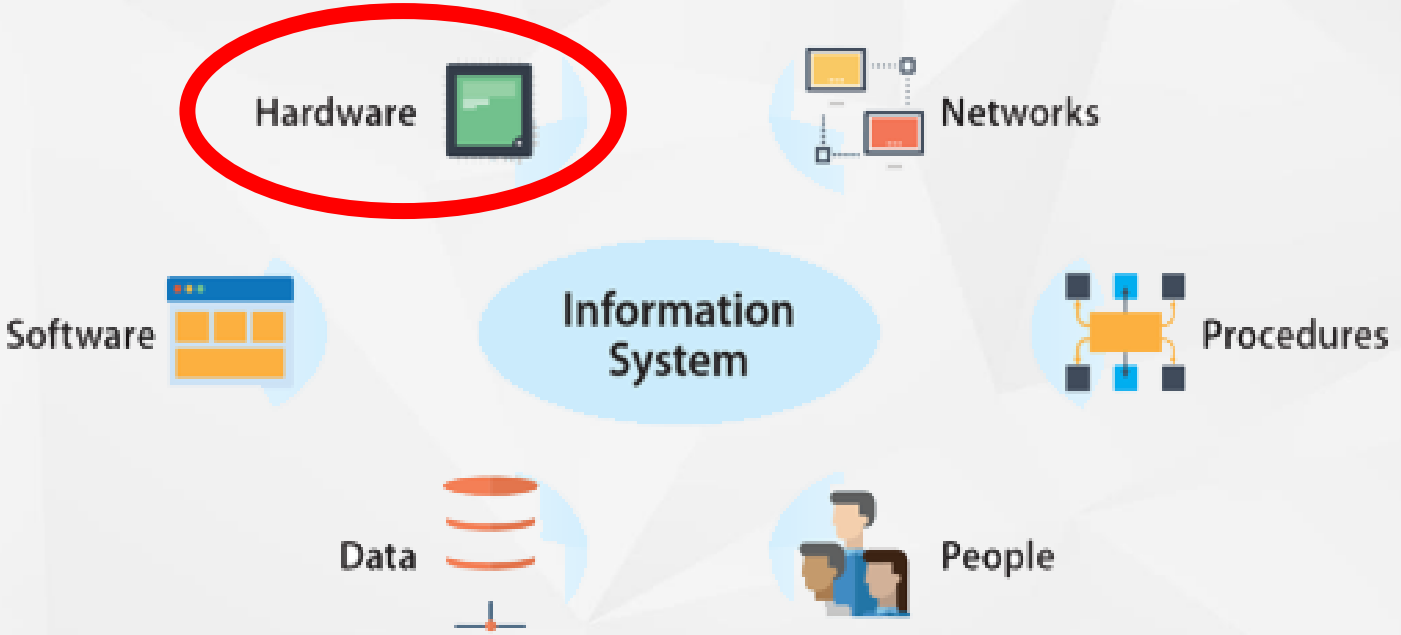
COMPONENTS OF AN INFORMATION SYSTEM

- Software - The software component of the IS comprises applications, operating systems, and assorted command utilities. Software is perhaps the 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



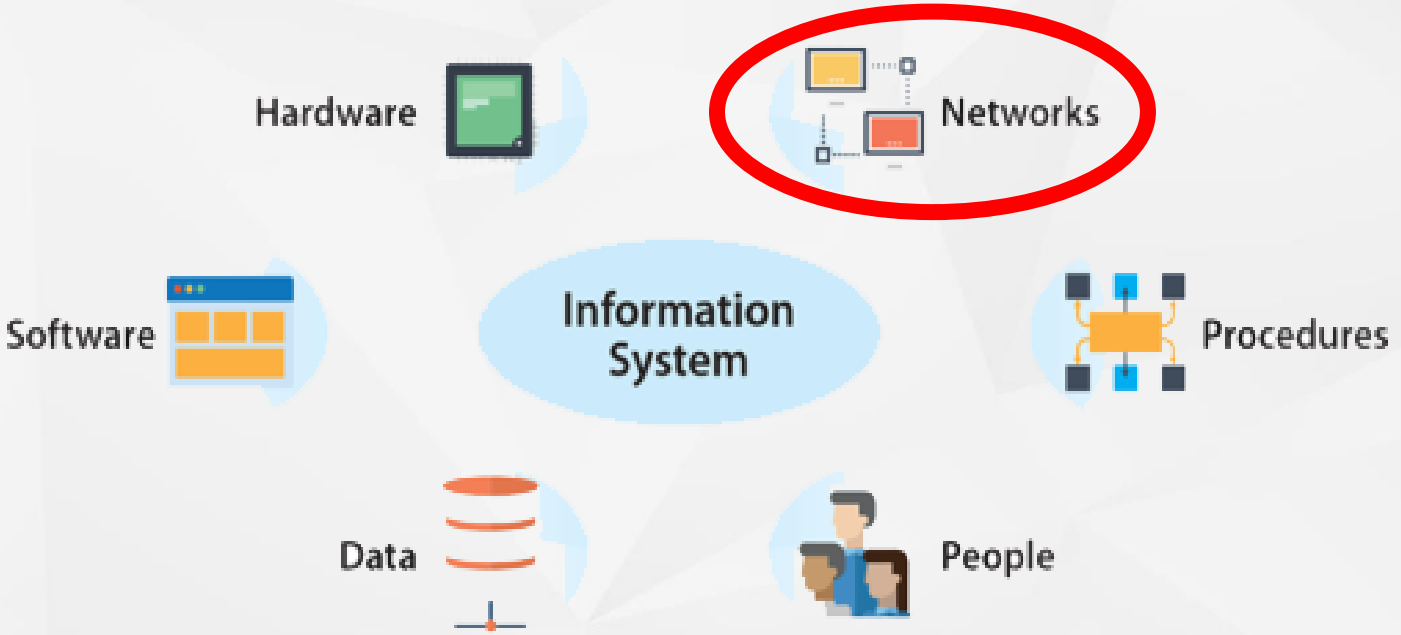
COMPONENTS OF AN INFORMATION SECURITY

- 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.



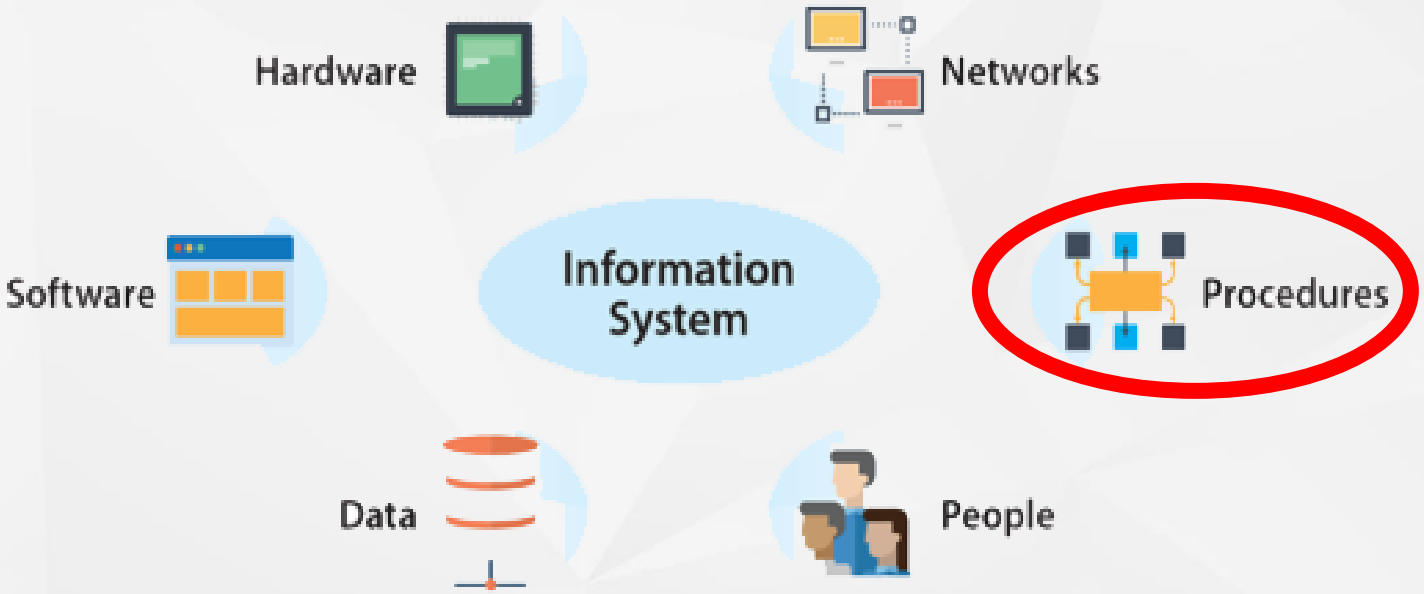
COMPONENTS OF AN INFORMATION SECURITY

- 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.



COMPONENTS OF AN INFORMATION SECURITY

- Procedures - Another frequently overlooked component of an IS is 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. 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.

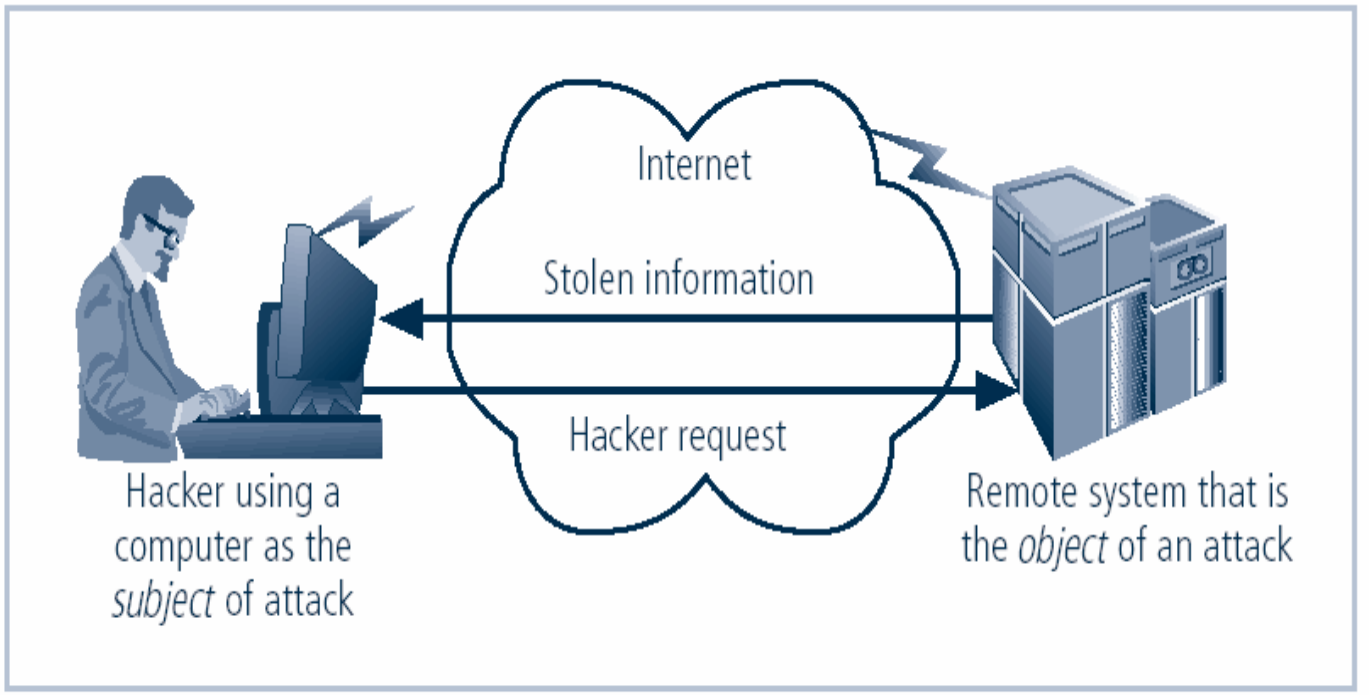


COMPONENTS OF AN INFORMATION SECURITY

- People - Though often overlooked in computer security considerations, people have always been a threat to information security. Legend has it that around 200 B.C. a great army threatened the security and stability of the Chinese empire. So ferocious were the invaders that the Chinese emperor commanded the construction of a great wall that would defend against the Hun invaders. Whether this event actually occurred or not, the moral of the story is that 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.

SECURING COMPONENTS

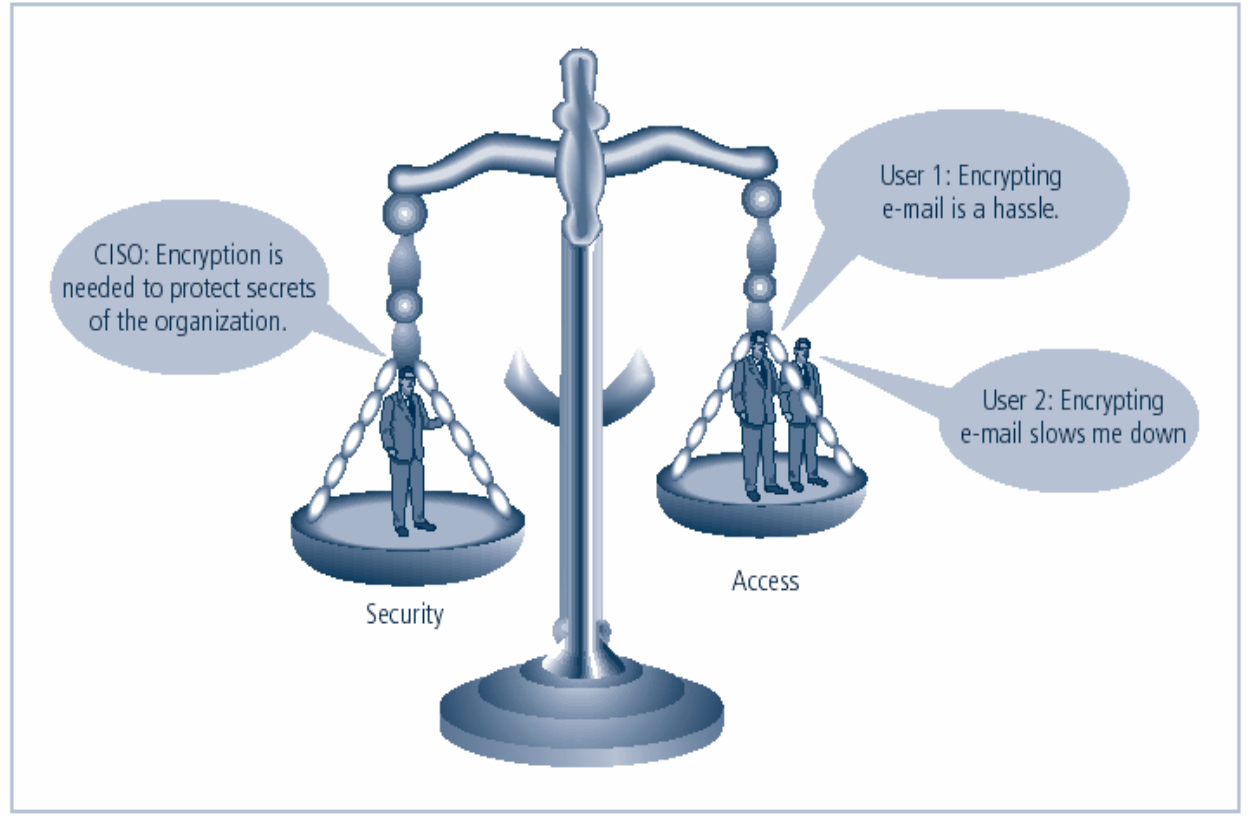
- Computer can be subject of an attack and/or the object of an attack
  - When the subject of an attack, computer is used as an active tool to conduct attack
  - When the object of an attack, computer is the entity being attacked



Computer as the Subject and Object of an Attack

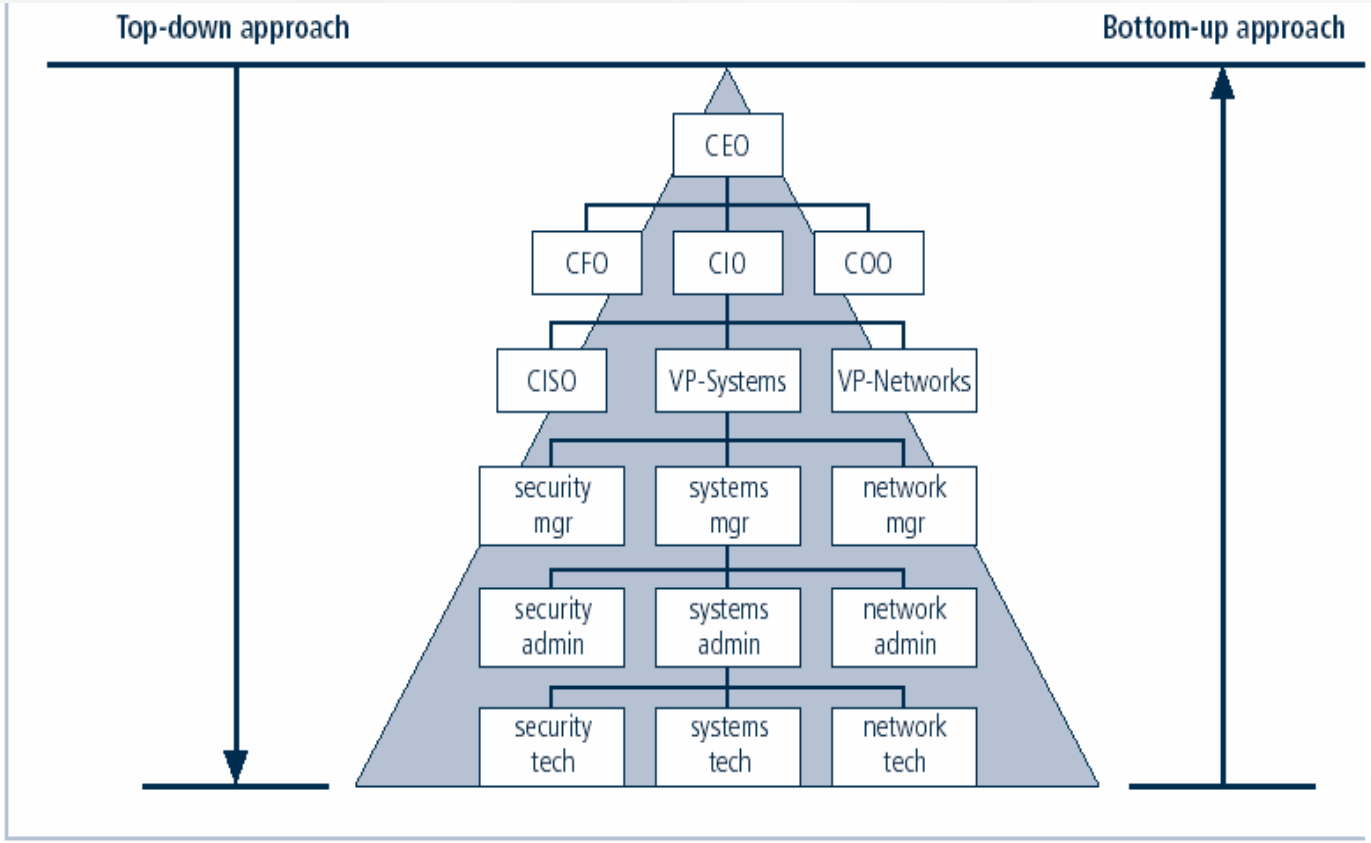
BALANCING INFORMATION SECURITY & ACCESS

- Impossible to obtain perfect security—it is a process, not an absolute
- Security should be considered balance between protection and availability
- To achieve balance, level of security must allow reasonable access, yet protect against threats



APPROACHES TO INFORMATION SECURITY IMPLEMENTATION: BOTTOM-UP APPROACH

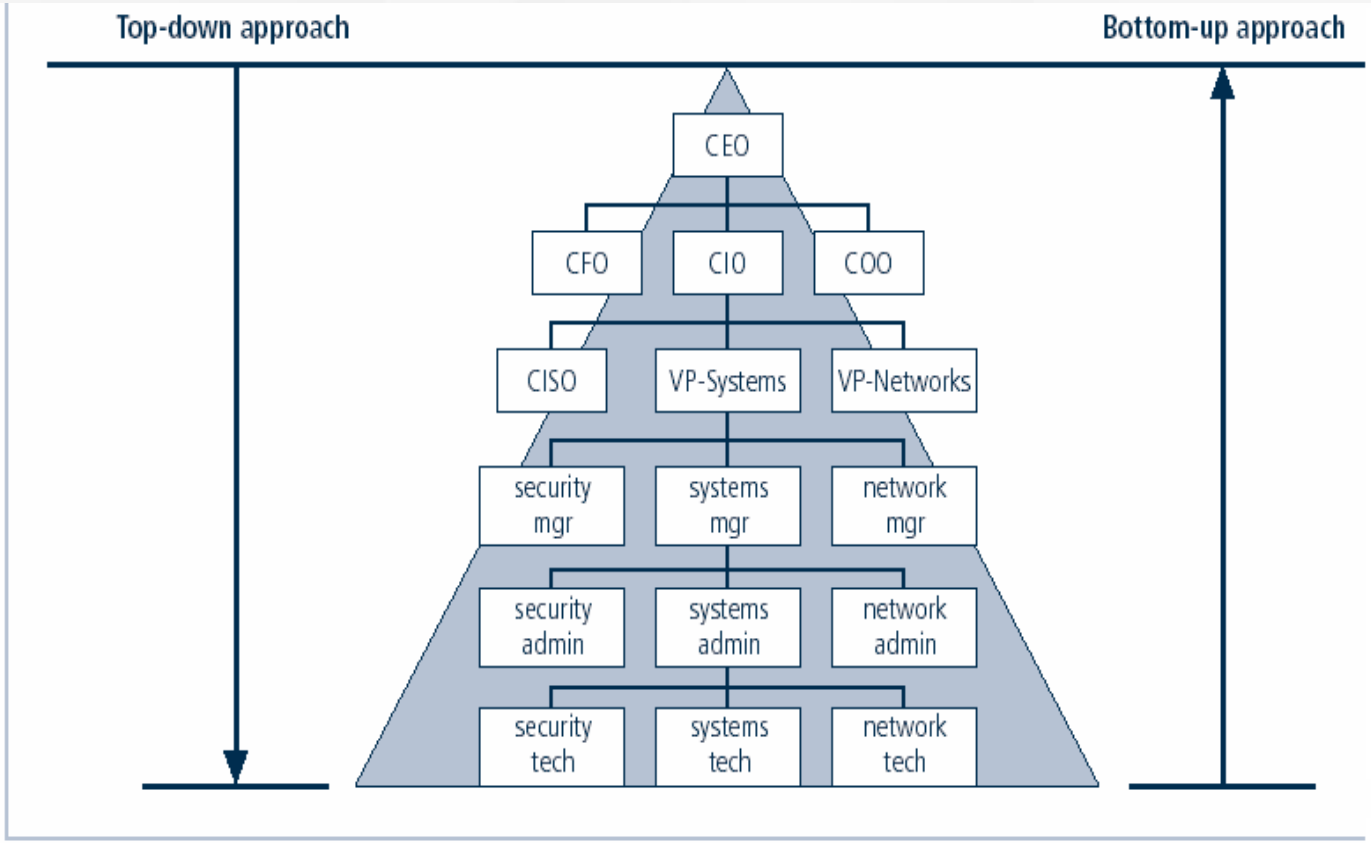
- Grassroots effort: systems administrators attempt to improve security of their systems
- Key advantage: technical expertise of individual administrators
- Seldom works, as it lacks a number of critical features:
  - Participant support
  - Organizational staying power



Approaches to Information Security Implementation

APPROACHES TO INFORMATION SECURITY IMPLEMENTATION: TOP-DOWN APPROACH

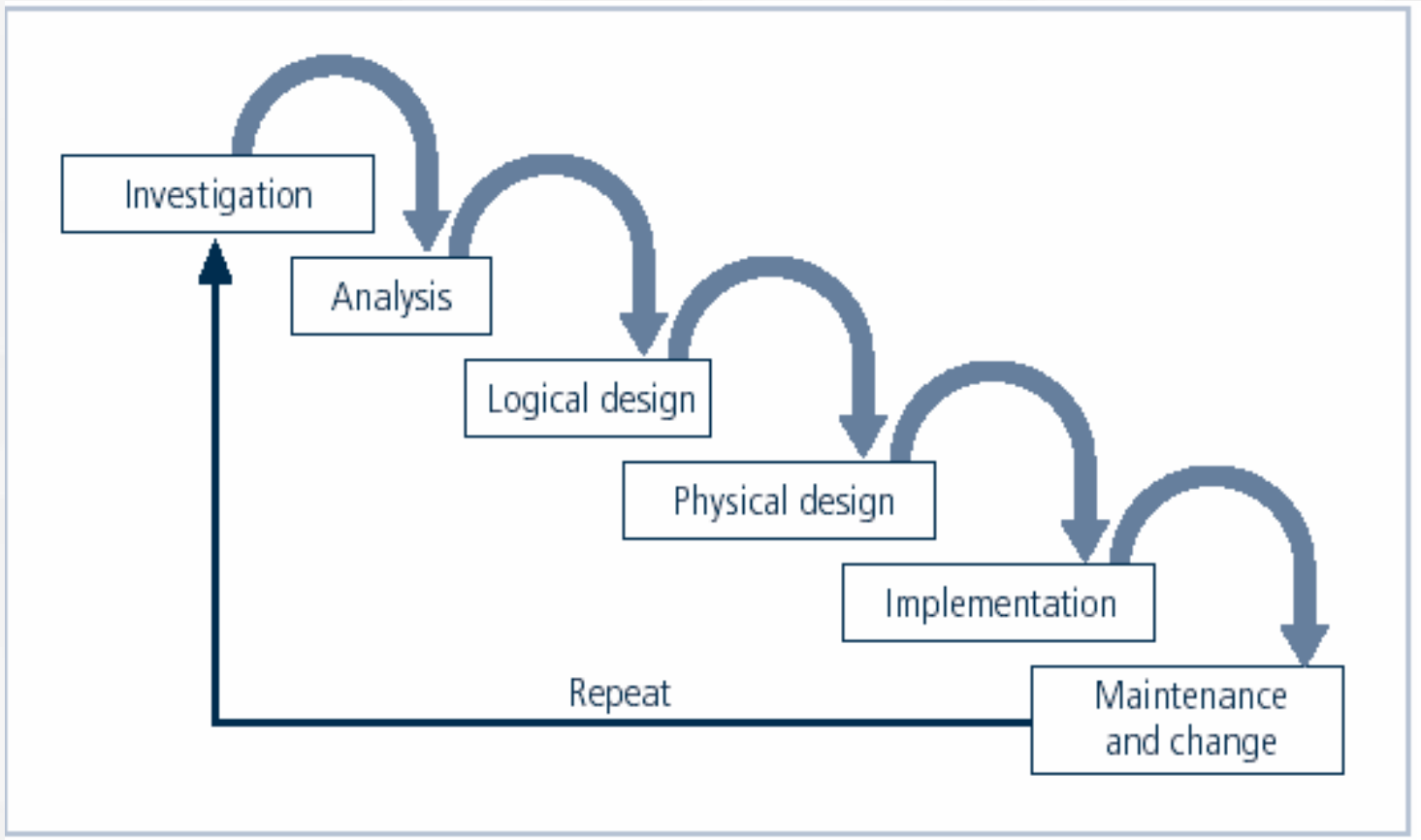
- Initiated by upper management
  - Issue policy, procedures and processes
  - Dictate goals and expected outcomes of project
  - Determine accountability for each required action
- The most successful also involve formal development strategy referred to as systems development life cycle



Approaches to Information Security Implementation

THE SYSTEMS DEVELOPMENT LIFE CYCLE

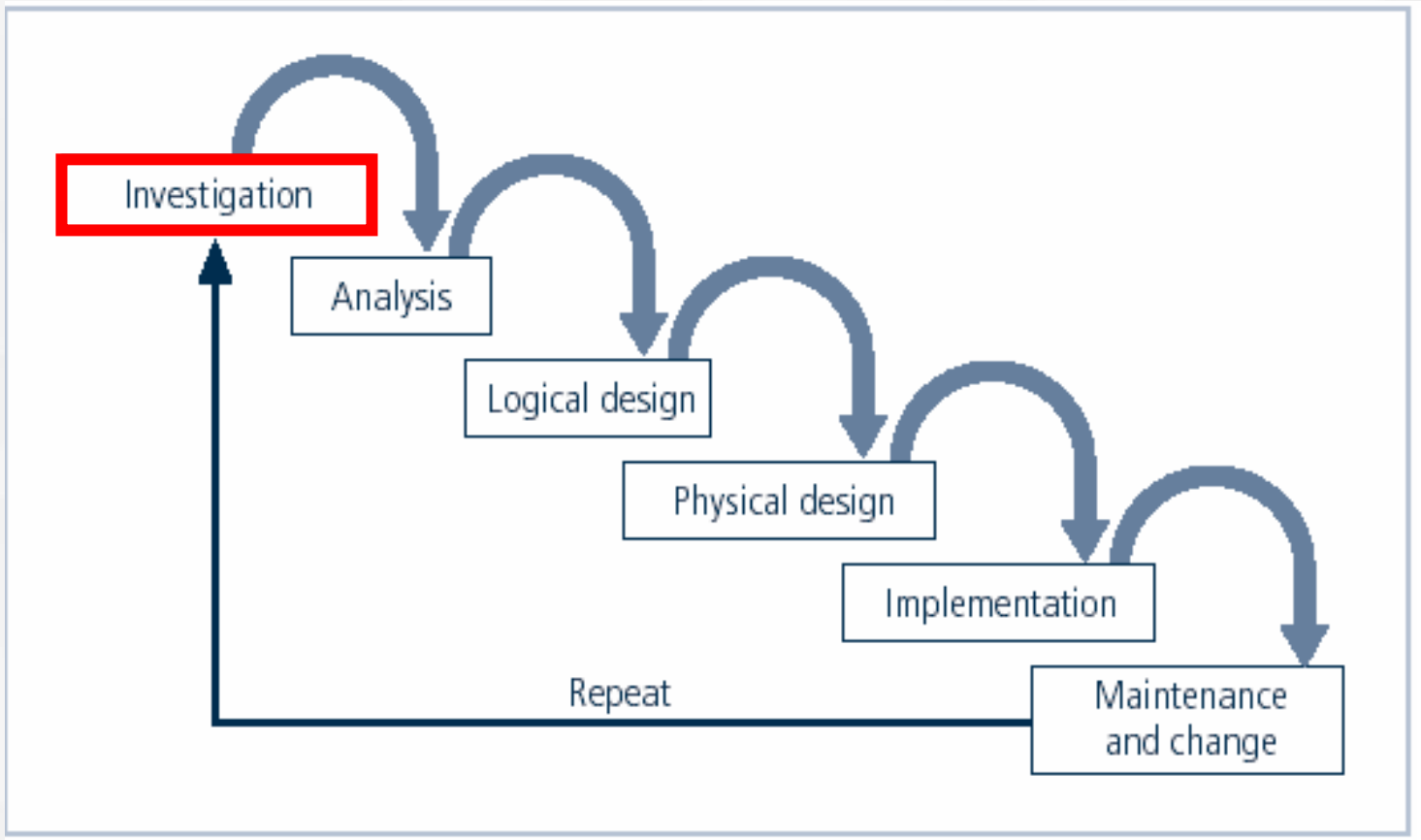
- Systems development life cycle (SDLC) is methodology and design for implementation of information security within an organization
- Methodology is formal approach to problem-solving based on structured sequence of procedures
- Using a methodology
  - ensures a rigorous process
  - avoids missing steps
- Goal is creating a comprehensive security posture/program
- Traditional SDLC consists of six general phases



SDLC Waterfall Methodology

THE SYSTEMS DEVELOPMENT LIFE CYCLE: INVESTIGATION

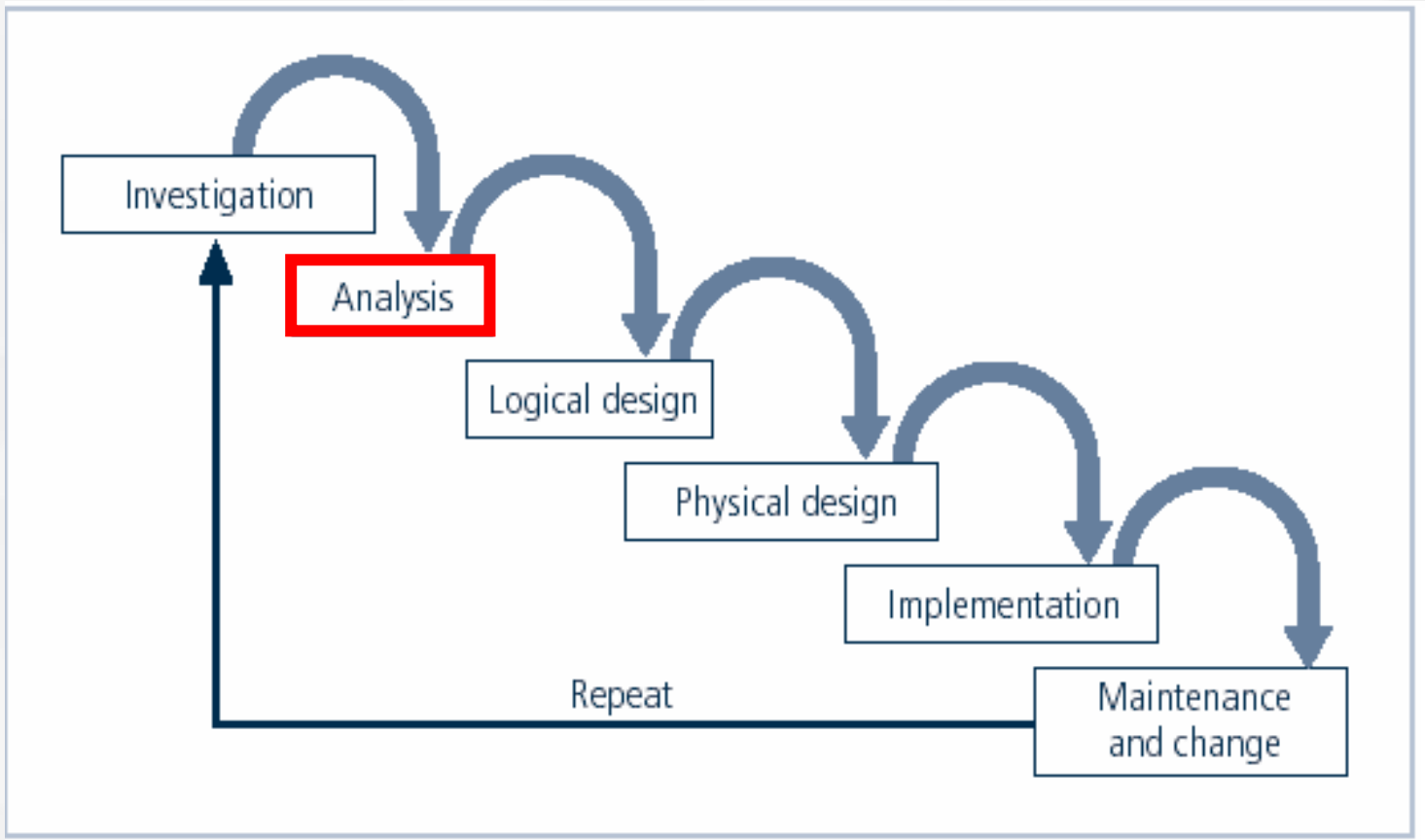
- What problem is the system being developed to solve?
- Objectives, constraints and scope of project are specified
- Preliminary cost-benefit analysis is developed
- At the end, feasibility analysis is performed to assesses economic, technical, and behavioral feasibilities of the process



SDLC Waterfall Methodology

THE SYSTEMS DEVELOPMENT LIFE CYCLE: ANALYSIS

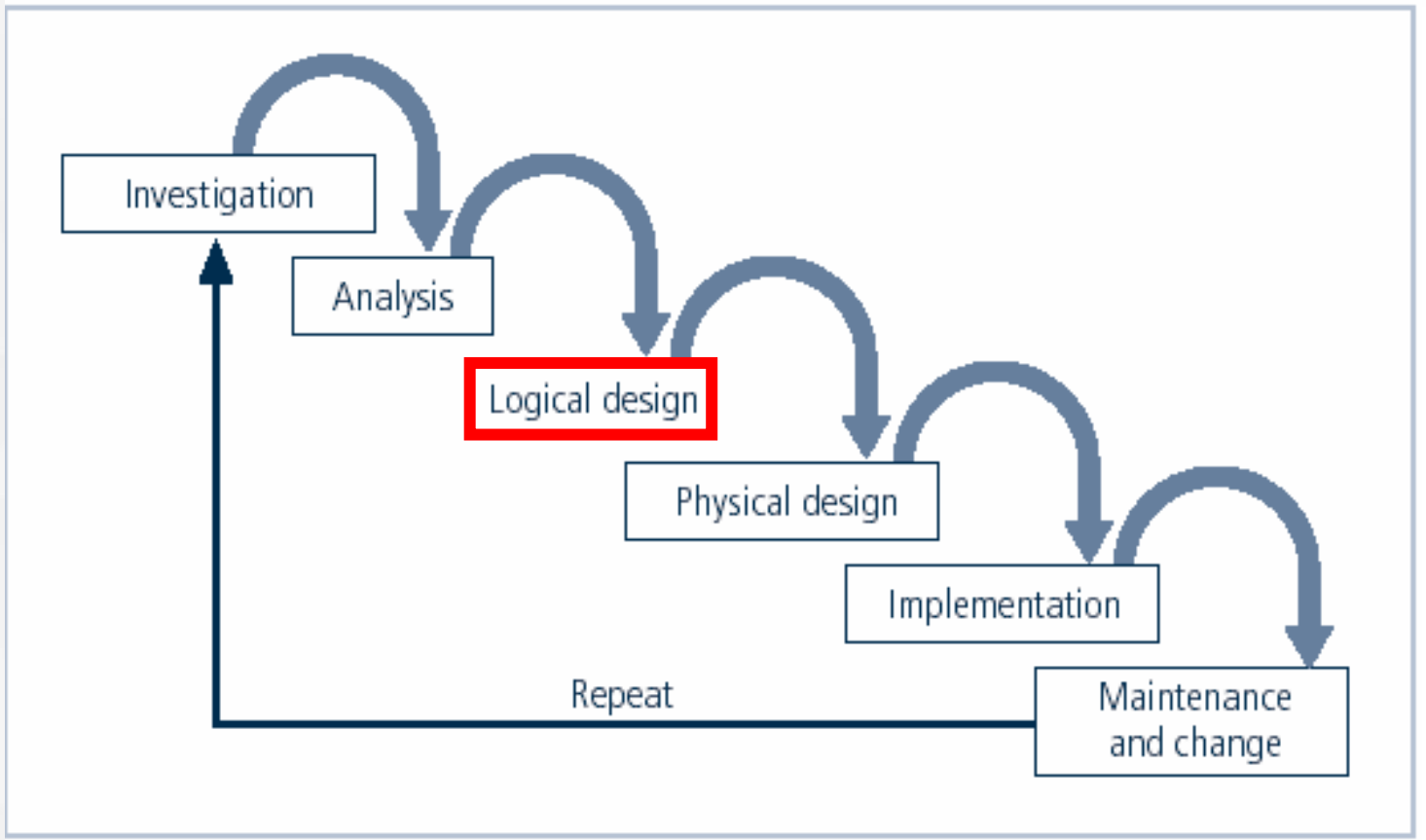
- Consists of assessments of the organization, status of current systems, and capability to support proposed systems
- Analysts determine what new system is expected to do and how it will interact with existing systems
- Ends with documentation of findings and update of feasibility analysis



SDLC Waterfall Methodology

THE SYSTEMS DEVELOPMENT LIFE CYCLE: LOGICAL DESIGN

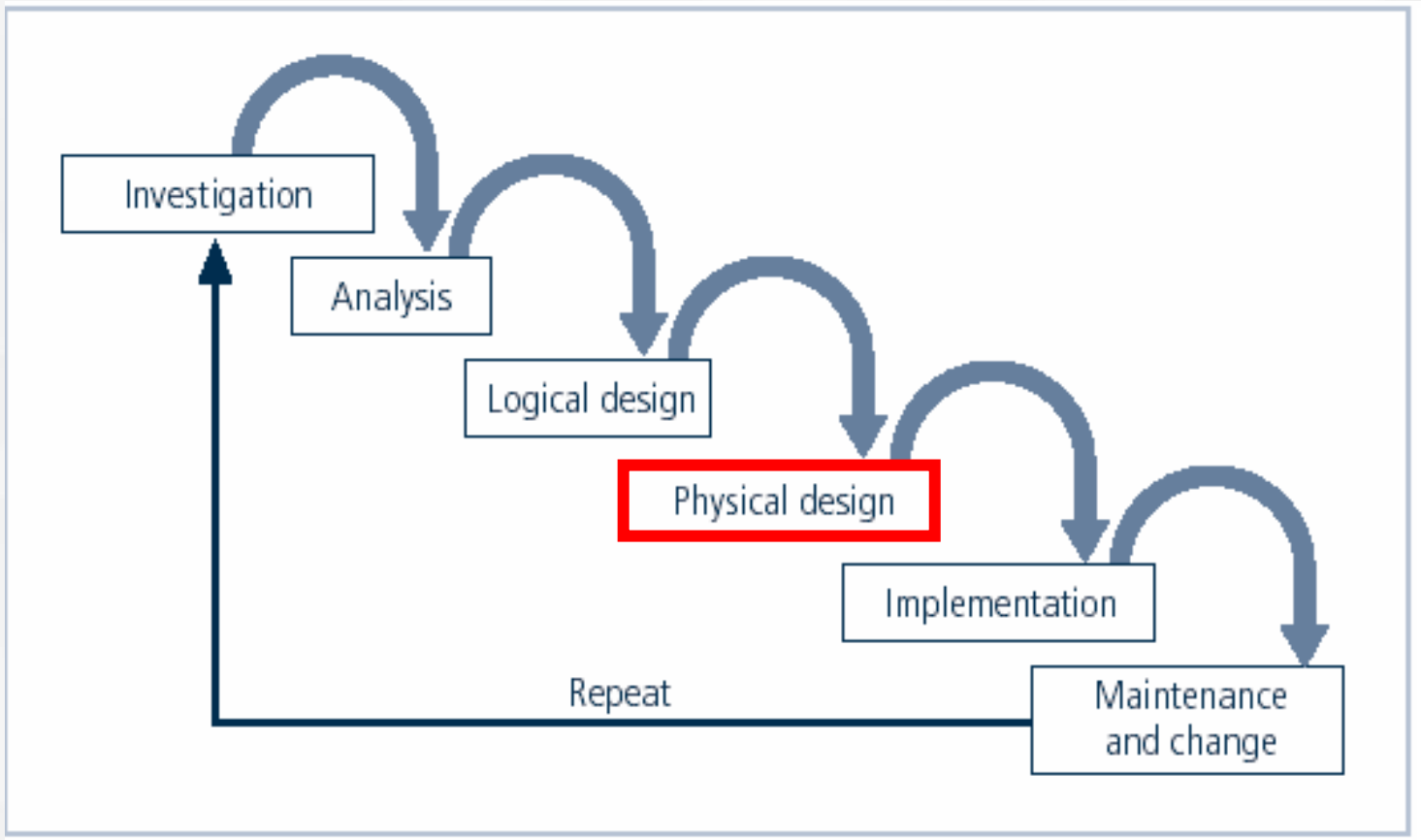
- Main factor is business need; applications capable of providing needed services are selected
- Data support and structures capable of providing the needed inputs are identified
- Technologies to implement physical solution are determined
- Feasibility analysis performed at the end



SDLC Waterfall Methodology

THE SYSTEMS DEVELOPMENT LIFE CYCLE: PHYSICAL DESIGN

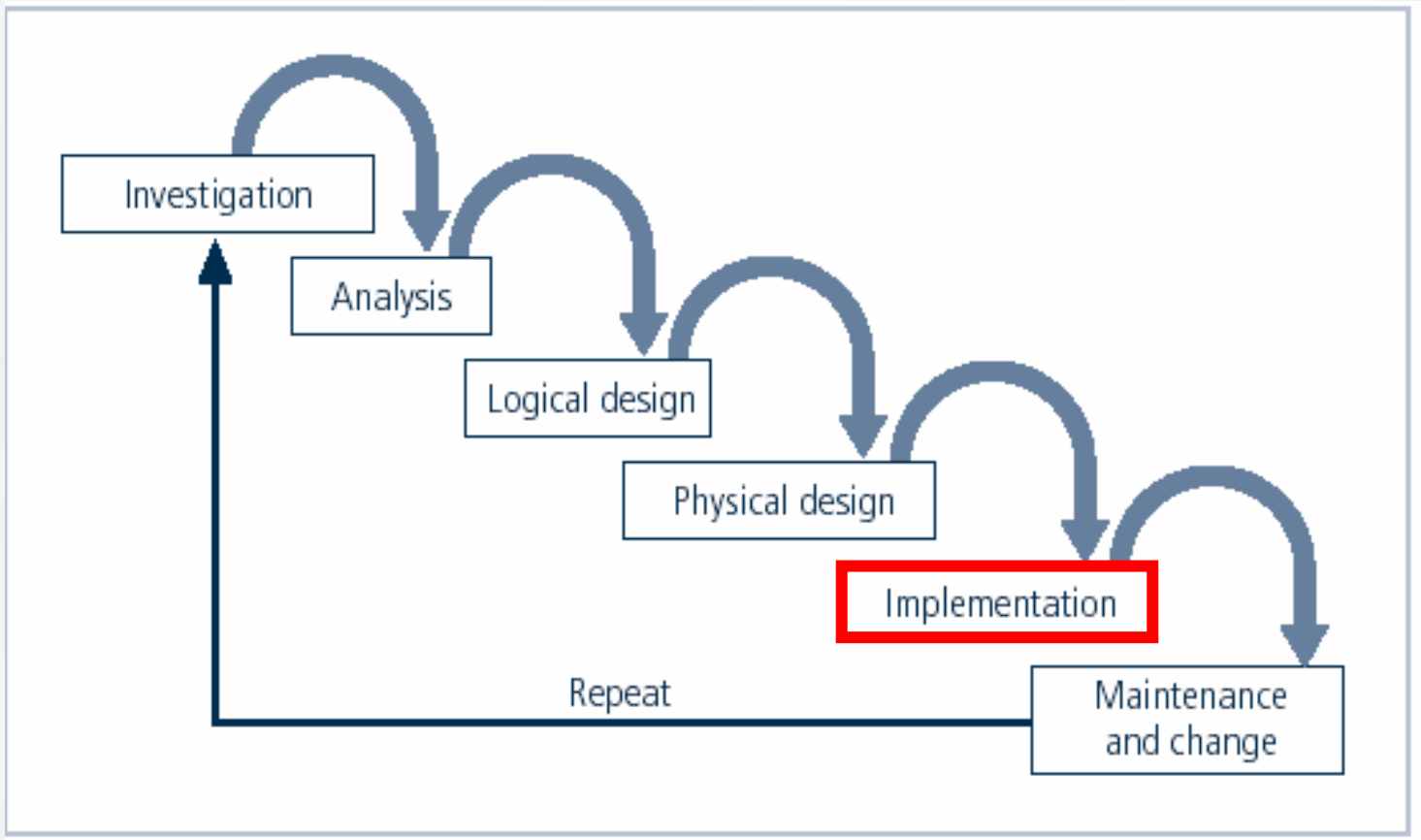
- Technologies to support the alternatives identified and evaluated in the logical design are selected
- Components evaluated on make-or-buy decision
- Feasibility analysis performed; entire solution presented to end-user representatives for approval



SDLC Waterfall Methodology

THE SYSTEMS DEVELOPMENT LIFE CYCLE: IMPLEMENTATION

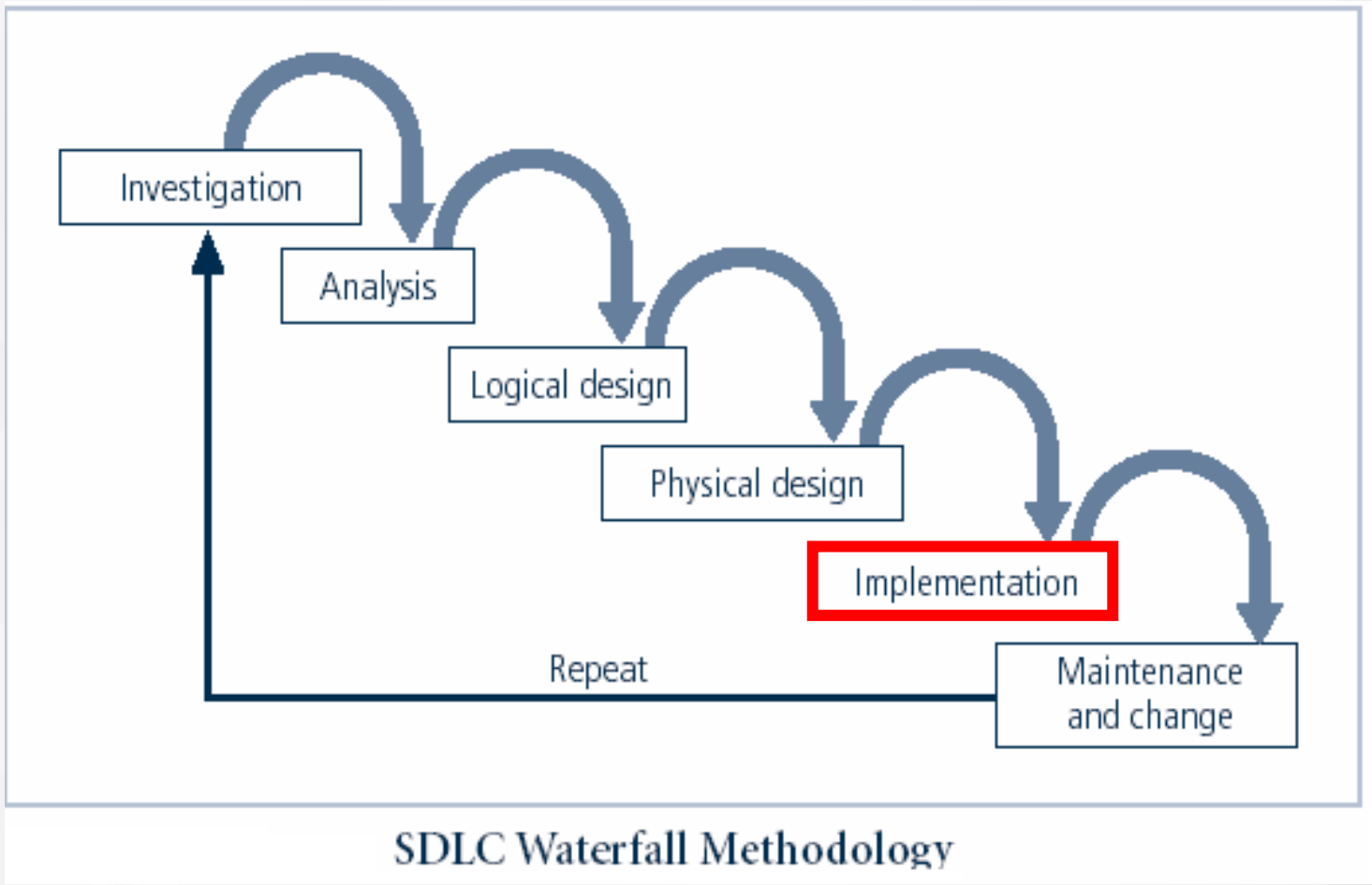
- Needed software created; components ordered, received, assembled, and tested
- Users trained and documentation created
- Feasibility analysis prepared; users presented with system for performance review and acceptance test



SDLC Waterfall Methodology

THE SYSTEMS DEVELOPMENT LIFE CYCLE: MAINTENANCE & CHANGE

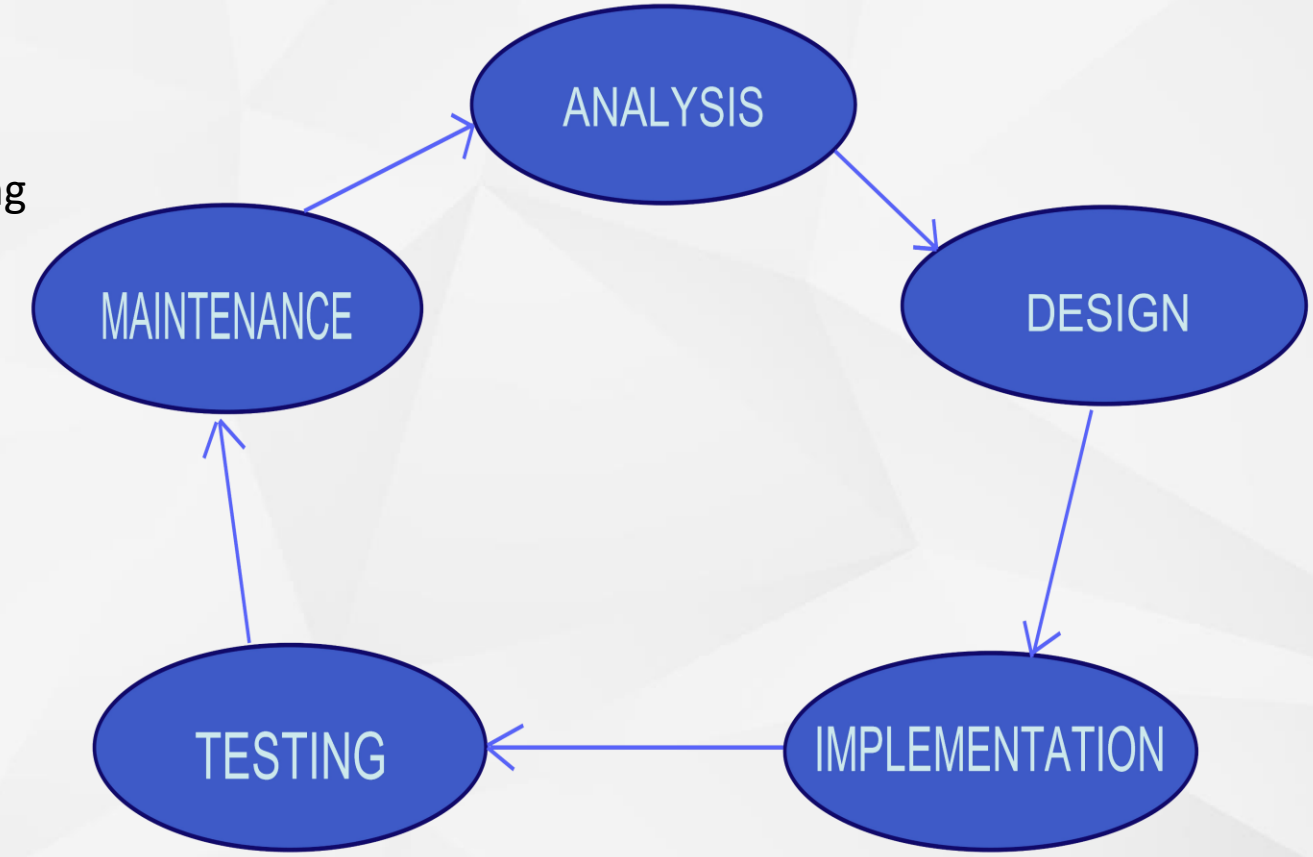
- Consists of tasks necessary to support and modify system for remainder of its useful life
- Life cycle continues until the process begins again from the investigation phase
- When current system can no longer support the organization's mission, a new project is implemented



SDLC Waterfall Methodology

THE SECURITY SYSTEMS DEVELOPMENT LIFE CYCLE

- The same phases used in traditional SDLC may be adapted to support specialized implementation of an IS project. While the two processes may differ in intent and specific activities, the overall methodology is the same. At its heart, implementing information security involves identifying specific threats and creating specific controls to counter those threats.
- Identification of specific threats and creating controls to counter them
- SecSDLC is a coherent program rather than a series of random, seemingly unconnected actions



THE SECURITY SYSTEMS DEVELOPMENT LIFE CYCLE

Investigation

- Identifies process, outcomes, goals, and constraints of the project
- Begins with enterprise information security policy
- Organizational feasibility analysis is performed

Analysis

- Documents from investigation phase are studied
- Analyzes existing security policies or programs, along with documented current threats and associated controls
- Includes analysis of relevant legal issues that could impact design of the security solution
- The risk management task begins

THE SECURITY SYSTEMS DEVELOPMENT LIFE CYCLE

Logical Design

- Creates and develops blueprints for information security
- Incident response actions planned:
  - Continuity planning
  - Incident response
  - Disaster recovery
- Feasibility analysis to determine whether project should continue or be outsourced

THE SECURITY SYSTEMS DEVELOPMENT LIFE CYCLE

Physical Design

- Needed security technology is evaluated, alternatives generated, and final design selected
- At end of the phase, a feasibility study determines readiness of organization for project

THE SECURITY SYSTEMS DEVELOPMENT LIFE CYCLE

Implementation

- Security solutions are acquired, tested, implemented, and tested again
- Personnel issues evaluated; specific training and education programs conducted
- Entire tested package is presented to management for final approval

Maintenance and Change

- Perhaps the most important phase, given the ever-changing threat environment
- Often, reparation and restoration of information is a constant duel with an unseen adversary
- Information security profile of an organization requires constant adaptation as new threats emerge and old threats evolve

SECURITY PROFESSIONALS & THE ORGANIZATION

- Wide range of professionals required to support a diverse information security program
- Senior management is key component; also, additional administrative support and technical expertise required to implement details of IS program

SENIOR MANAGEMENT

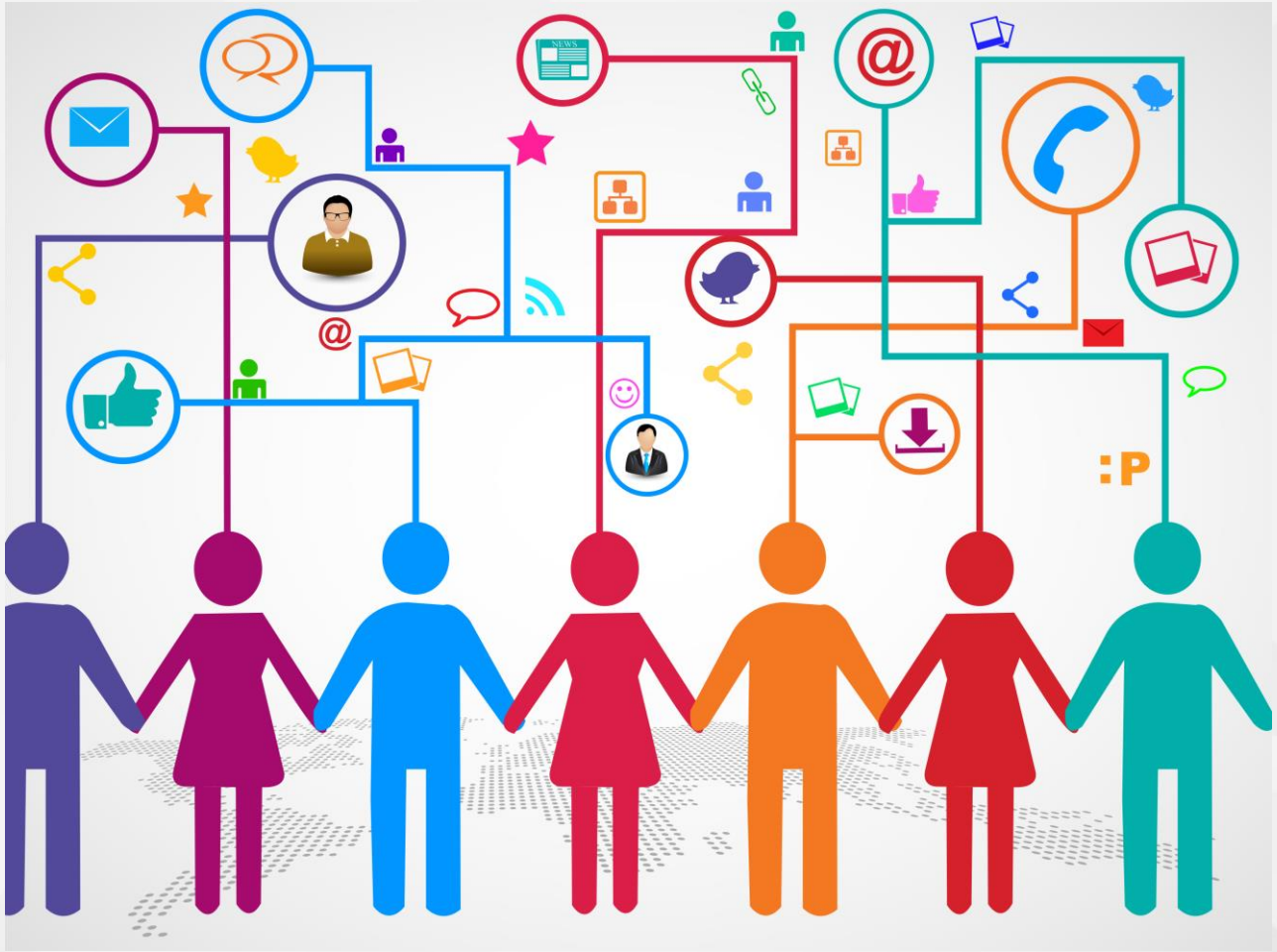
- Chief Information Officer (CIO)
  - Senior technology officer
  - Primarily responsible for advising senior executives on strategic planning
- Chief Information Security Officer (CISO)
  - Primarily responsible for assessment, management, and implementation of IS in the organization
  - Usually reports directly to the CIO

INFORMATION SECURITY PROJECT TEAM

- A number of individuals who are experienced in one or more facets of technical and non-technical areas:
  - Champion
  - Team leader
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems administrators
  - End users

DATA RESPONSIBILITIES

- Data Owner: responsible for the security and use of a particular set of information
- Data Custodian: responsible for storage, maintenance, and protection of information
- Data Users: end users who work with information to perform their daily jobs supporting the mission of the organization



KEY INFORMATION SECURITY CONCEPTS

● **Protection** profile or security posture: The entire set of controls and safeguards, including policy, education, training and awareness, and technology, that the organization implements (or fails to implement) to protect the asset. The terms are sometimes used interchangeably with the term security program, although the security program often comprises managerial aspects of security, including planning, personnel, and subordinate programs.
● **Risk**: The probability that something unwanted will happen. Organizations must minimize risk to match their risk appetite—the quantity and nature of risk the organization is willing to accept.
● Subjects and objects: A computer can be either the subject of an attack—an agent entity used to conduct the attack—or the object of an attack—the target entity.
● **Threat**: A category of objects, persons, or other entities that presents a danger to an asset. Threats are always present and can be purposeful or undirected. For example, hackers purposefully threaten unprotected information systems, while severe storms incidentally threaten buildings and their contents.
● **Threat agent**: The specific instance or a component of a threat. For example, all hackers in the world present a collective threat, while Kevin Mitnick, who was convicted for hacking into phone systems, is a specific threat agent. Likewise, a lightning strike, hailstorm, or tornado is a threat agent that is part of the threat of severe storms.
● **Vulnerability**: A weaknesses or fault in a system or protection mechanism that opens it to attack or damage. Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door. Some well-known vulnerabilities have been examined, documented, and published; others remain latent (or undiscovered).

KEY INFORMATION SECURITY CONCEPTS

● **Access**: A subject or object's ability to use, manipulate, modify, or affect another subject or object. Authorized users have legal access to a system, whereas hackers have illegal access to a system. Access controls regulate this ability.
● **Asset**: The organizational resource that is being protected. An asset can be logical,
such as a Web site, information, or data; or an asset can be physical, such as a person, computer system, or other tangible object. Assets, and particularly information assets, are the focus of security efforts; they are what those efforts are attempting to protect.
● **Attack**: An intentional or unintentional act that can cause damage to or otherwise compromise information and/or the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect.
● Control, safeguard, or countermeasure: Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve the security within an organization.
● **Exploit**: A technique used to compromise a system. This term can be a verb or a noun. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain. Or, an exploit can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or is created by the attacker. Exploits make use of existing software tools or custom-made software components.
● **Exposure**: A condition or state of being exposed. In information security, exposure exists when a vulnerability known to an attacker is present.
● **Loss**: A single instance of an information asset suffering damage or unintended or unauthorized modification or disclosure. When an organization's information is stolen, it has suffered a loss.

SUMMARY

- Information security is a “well-informed sense of assurance that the information risks and controls are in balance.”
- Computer security began immediately after first mainframes were developed
- Successful organizations have multiple layers of security in place: physical, personal, operations, communications, network, and information.
- Security should be considered a balance between protection and availability
- Information security must be managed similar to any major system implemented in an organization using a methodology like SecSDLC

QUIZ #1

INSTRUCTIONS:

Provide brief answers to the following review questions.

1. What is the difference between a threat agent and a threat?
2. What is the difference between vulnerability and exposure?
3. How is infrastructure protection (assuring the security of utility services) related to information security?
4. What type of security was dominant in the early years of computing?
5. What are the three components of the C.I.A. triangle? What are they used for?
6. Describe the critical characteristics of information. How are they used in the study of computer security?
7. Identify the six components of an information system. Which are most directly affected by the study of computer security? Which are most commonly associated with its study?
8. Why is the top-down approach to information security superior to the bottom-up approach?
9. Why is a methodology important in the implementation of information security? How does a methodology improve the process?

10 Which members of an organization are involved in the security system development life cycle? Who leads the process?