Lesson 1:
Information Security

Introduction to Information Security

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Define information security
- Recount the history of computer security, and explain how it evolved into information security
- Define key terms and critical concepts of information security
- Explain the role of security in the systems development life cycle
- Describe the information security roles of professionals within an organization

The History of Information Security

Homework:

Please, write about the history of information security.

- NB: Should not be more than three pages.

1. What is security?

Security: protecting general assets

Security can be realized through:

1. Prevention: take measures that stop assets from being damaged.

2. Detection: take measures so that you can know when, how, and by whom an asset has been damaged.

3. Reaction: take measures so that you can recover your assets or to recover from a damage to your assets

- Examples: next slide
- There are many branches of Security: national security, economic security, *information security*, etc.

Examples

Ex. 1 - Private property

– Prevention: locks at doors, window bars, walls around the property.

– Detection: stolen items aren’t there any more, burglar alarms, CCTV, …

– Reaction: call the police,…

Examples

Ex. 2 - eCommerce

– Prevention: encrypt your orders, rely on the merchant to perform checks on the caller,…

– Detection: an unauthorized transaction appears on your credit card Statement.

– Reaction: complain, ask for a new credit card number, …

Computer Security Vs. Network Security

- **Computer security** involves implementing measures to secure a single computer.
- When securing a single computer, you are concerned with protecting the resources stored on that computer and protecting that computer from threats.
- **Network security** involves protecting all the resources on a network from threats.

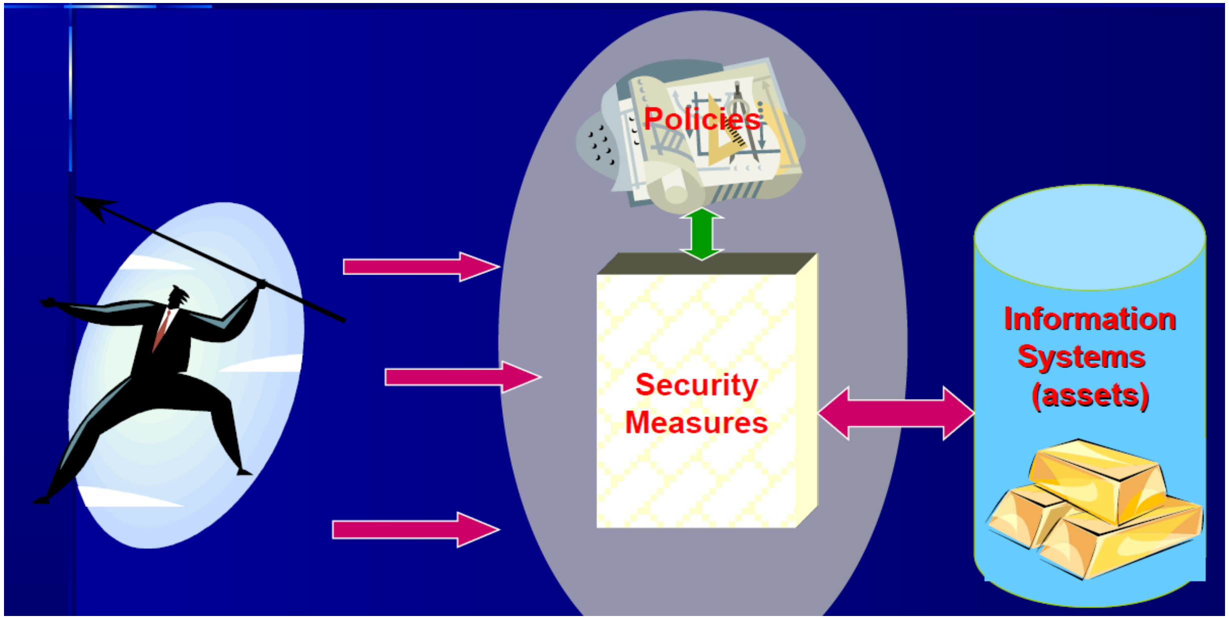
2. What is Information Security?

- ***Information security*:** is concerned with protecting information and information resources such as: books, faxes, computer data, voice communications, etc.

Information security is determining:

- *what* needs to be protected, *i.e.*, assets
- and *why* (Security requirements which include CIA),
- *what* needs to be protected from (Threats, vulnerabilities, risks),
- and *how* (Security measures) to protect it for as long as it exists
- – Security measures which are implemented according to a security policy

3. What is Information System Security (ISS)?



Attackers

Information System Security

- ISS is concerned with protecting Information system assets such as PCs, software, applications, etc.
- In order to ensure the security of Information Systems, we need to determine:

1. Assets (i.e., Information systems) to be protected
2. Security requirements; CIA
3. Threats, vulnerabilities, risks
4. Security policies
5. Security measures

Components of an Information System

- Information system (IS) is entire set of components necessary to use information as a resource in the organization
  - Software
  - Hardware
  - Data
  - People
  - Procedures
  - Networks

Components of an Information System

- An information system (IS) is much more than computer hardware; it is the entire set of people, procedures, and technology that enable business to use information.
- The six critical components are: hardware, software, networks, people, procedures, and data 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 IS also has its own security requirements.

Software

- The software component of an IS includes applications (programs), 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 (IT) 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.

Example of Information System

People

Source: shapecharge

Hardware

Source: 4X-image

Software

Source: Ali Kerem Yucel

Networks

Source: Ovchinnkov Vladimir

Data

Source: NAN104

Procedures

Source: Mark Agnor

Source: Pinkypills

Components of an Information System

Software – Cont’d

- Software carries the lifeblood of information through an organization.
- Unfortunately, software programs are often created under the constraints of project management, which limit time, costs, and manpower.
- Information security is all too often implemented as an afterthought rather than developed as an integral component from the beginning. In this way, software programs become an easy target of accidental or intentional attacks.

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 hardware access is possible.

Data

- Data stored, processed, and transmitted by a computer system must be protected.
- Data is often the most valuable asset of an organization and therefore is the main target of intentional attacks.
- Systems developed in recent years are likely to make use of database management systems. When used properly, they should improve the security of the data and the applications that rely on the data.
- 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 make them less secure than traditional file systems.
- Because data and information exist in physical form in many organizations as paper reports, handwritten notes, and computer printouts, the protection of physical information is as important as the protection of electronic, computer-based information.
- As an aside, the terms data and information are used interchangeably today.

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.
- 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 people to obtain access information about a system.

Procedures

- Procedures are another frequently overlooked component of an IS. Procedures are written instructions for accomplishing a specific task.
- When an unauthorized user obtains an organization’s procedures, it 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), the bank consultant ordered millions of cedis to be transferred by wire to his own account.

Networks

- Networking is the IS component that created much of the need for increased computer and information security.
- When information systems are connected to each other to form LANs, and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge.
- Applying the traditional tools of physical security, such as locks and keys, to restrict access to the system’s hardware components is still important.
- However, when computer systems are networked, this approach is no longer enough.
- Steps to provide network security such as installing and configuring firewalls are essential, as is implementing intrusion detection systems to make system owners aware of ongoing compromises.

What is Security? – Cont’d

- In general, security is “the quality or state of being secure--to be free from danger.”
- It means to be protected from adversaries--from those who would do harm, intentionally or otherwise.
- A successful organization should have the following multiple layers of security in place for the protection of its operations:
  - Physical security – To protect the physical items, objects, or areas of an organization from unauthorized access and misuse.
  - Personal security – To protect the individual or group of individuals who are authorized to access the organization and its operations.
  - Operations security – To protect the details of a particular operation or series of activities.
  - Communications security – To protect an organization’s communications media, technology, and content.
  - Network security – To protect networking components, connections, and contents.

Components of information security

- Figure 1 shows that information security includes the broad areas of information security management, data security, and network security.

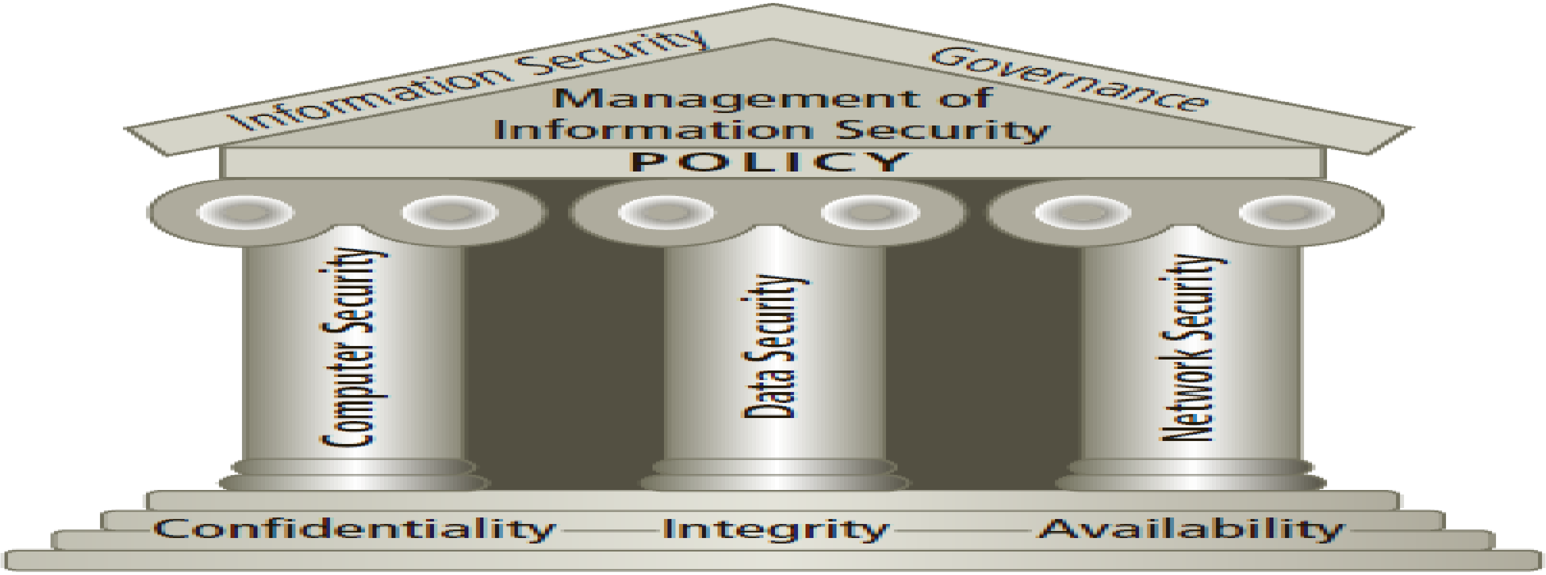


Figure1: Components of information security

The C.I.A. triad

- The C.I.A. triad (see Figure 2) has been the standard for computer security in both industry and government since the development of the computer.
- This standard is based on the **three characteristics** of information that give it value to organisations: **confidentiality, integrity, and availability**.

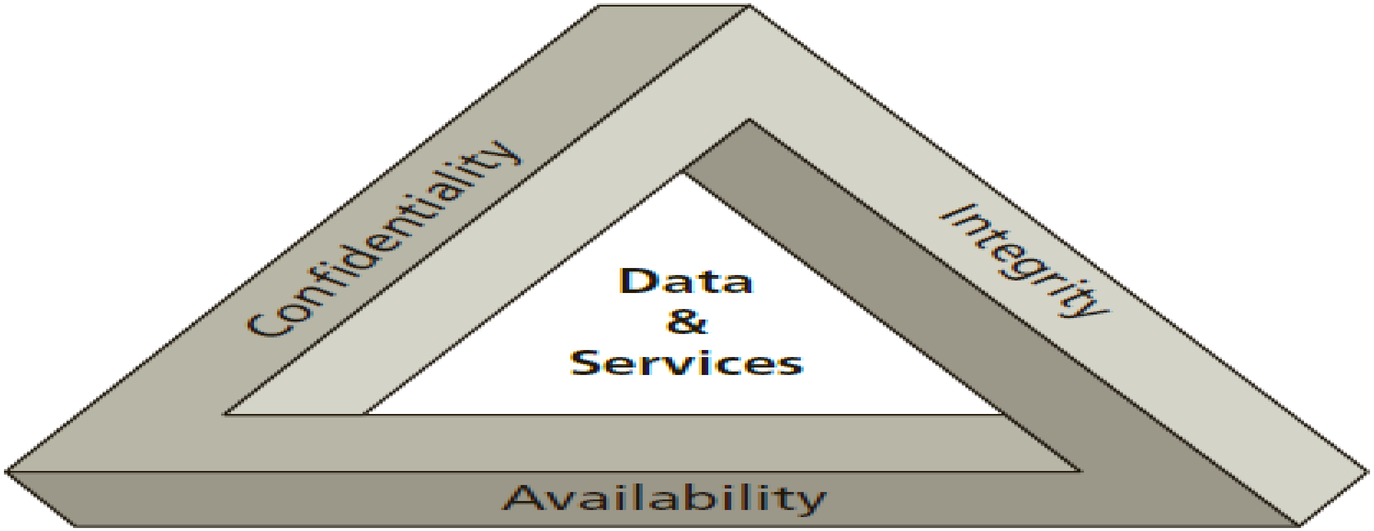


Figure 2: The C.I.A. triad

Introduction - **What Is Information Security?**

- Information security: a "well-informed sense of assurance that the information risks and controls are in balance." — Jim Anderson, Inovant (2002)
- Security professionals must review the origins of this field to understand its impact on our understanding of information security today

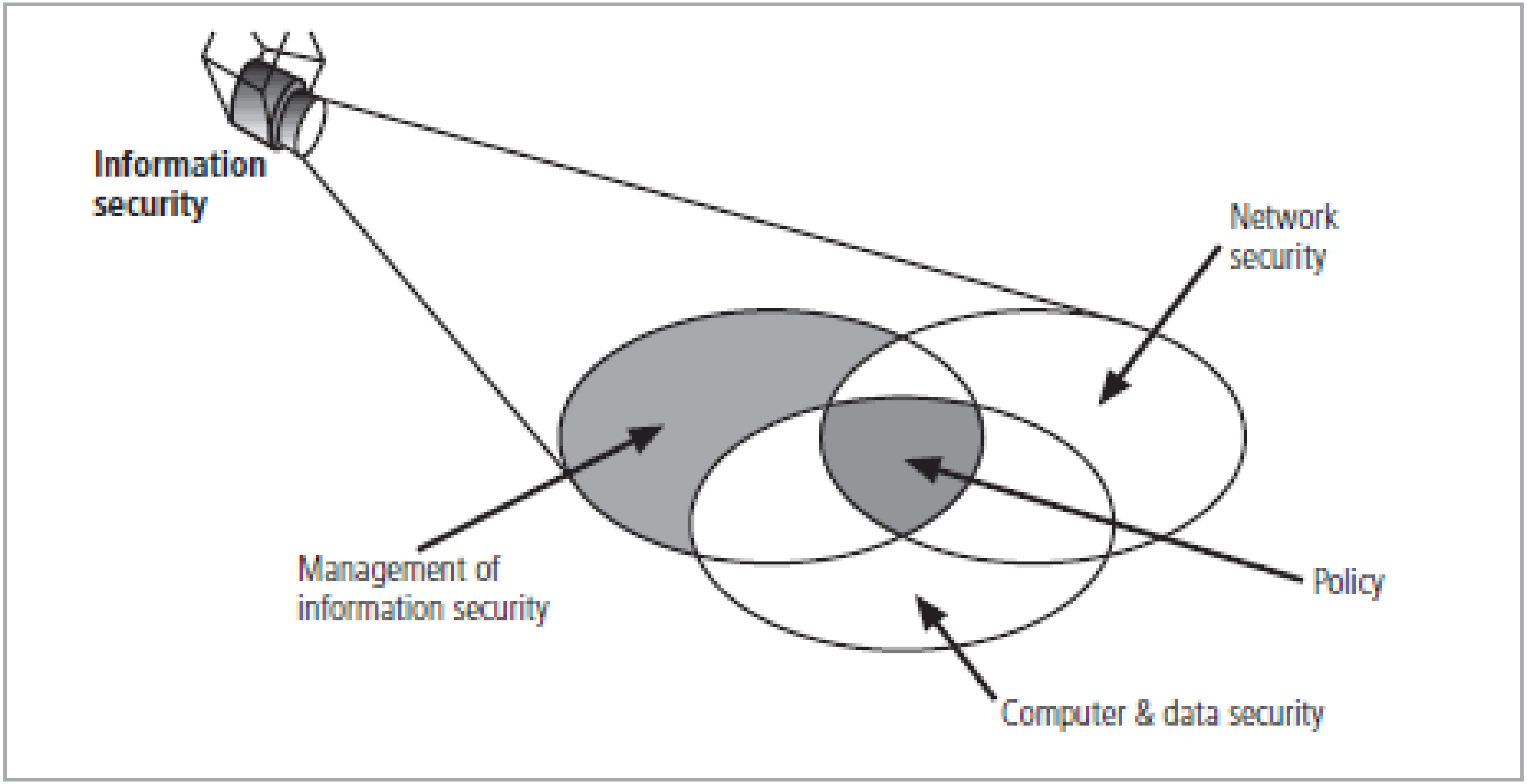


Figure Components of Information Security

Key Information Security Concepts

- Access
- Asset
- Attack
- Control, Safeguard, or Countermeasure
- Exploit
- Exposure
- Loss
- Protection Profile or Security Posture
- Risk
- Subjects and Objects
- Threat
- Threat Agent
- Vulnerability

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 that is being protected.
- Attack - an act that is an intentional or unintentional attempt to cause damage or compromise to the information and/or the systems that support it.
- 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 - to take advantage of weaknesses or vulnerability in a system.
- Exposure - a single instance of being open to damage.
- Hack - Good: to use computers or systems for enjoyment; Bad: to illegally gain access to a computer or system.
- Object - a passive entity in the information system that receives or contains information.

Example of Asset

Assets have to be identified and value. In an IT system assets include:

- Hardware: laptops, severs, routers, PDAs, mobile phones, smart cards, etc.
- Software: applications, operating systems, database management systems, source code, object code, etc.
- Data and information: essential data for running and planning the business, design documents, digital content, data about your customers, etc.
- Reputation: the beliefs or opinions that are generally held about someone or something; eg. His reputation was tarnished by allegations of bribery.

Key Information Security Concepts

- Risk - the probability that something can happen.
- Security Blueprint - the plan for the implementation of new security measures in the organization.
- Security Model - a collection of specific security rules that represents the implementation of a security policy.
- Security Posture or Security Profile - a general label for the combination of all policies, procedures, technologies, and programs that make up the total security effort currently in place.
- Subject - an active entity that interacts with an information system and causes information to move through the system for a specific end purpose

Key Information Security Concepts

- Threats - a category of objects, persons, or other entities that represents a potential danger to an asset.
- Threat Agent - a specific instance or component of a more general threat.
- Vulnerability - weaknesses or faults in a system or protection mechanism that expose information to attack or damage. is a weakness in system design or implementation and can be in hardware or software.

Example: a software bug exists in the OS, or no password rules are set.

Or an unlocked door.

Example of Vulnerability:

- Accounts with system privileges where the default password, such as

‘MANAGER’, has not been changed.

- Programs with unnecessary privileges.
- Programs with known flaws.
- Weak access control settings on resources, for example, granting everyone full control to a shared folder.
- Weak firewall configurations that allow access to vulnerable services.

Vulnerability scanners

- **Vulnerability scanners** (also called **risk analysis tools**) provide a systematic and automated way of identifying vulnerabilities. However, their knowledge base of known vulnerabilities has to be kept up to date. Organizations like the Computer Emergency Response Team (CERT) provide this information, as do security advisories of software companies. One vulnerability scanner provided by Microsoft® is the Microsoft Baseline Security Analyzer (MBSA).
- Vulnerabilities can be rated according to their impact (level of criticality). A vulnerability that allows an attacker to take over an administrator account is more critical than a vulnerability that gives access to an unprivileged user account.

Vulnerability scanners – Cont’d

- Vulnerabilities can be rated according to their impact (level of criticality). A vulnerability that allows an attacker to take over an administrator account is more critical than a vulnerability that gives access to an unprivileged user account.
- A vulnerability that allows an attacker to completely impersonate a user is more critical than a vulnerability that allows a user to be impersonated only in the context of a single specific service. Some vulnerability scanners give a rating for the vulnerabilities they detect.

Key Information Security Concepts (cont'd.)

- Computer can be subject of an attack
- Computer can be 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

Key Information Security Concepts

- When considering the security of information systems components, it is important to understand the concept of the computer as the subject of an attack as opposed to the computer as the object of an attack.
- When a computer is the subject of an attack, it is used as an active tool to conduct the attack. When a computer is the object of an attack, it is the entity being attacked.

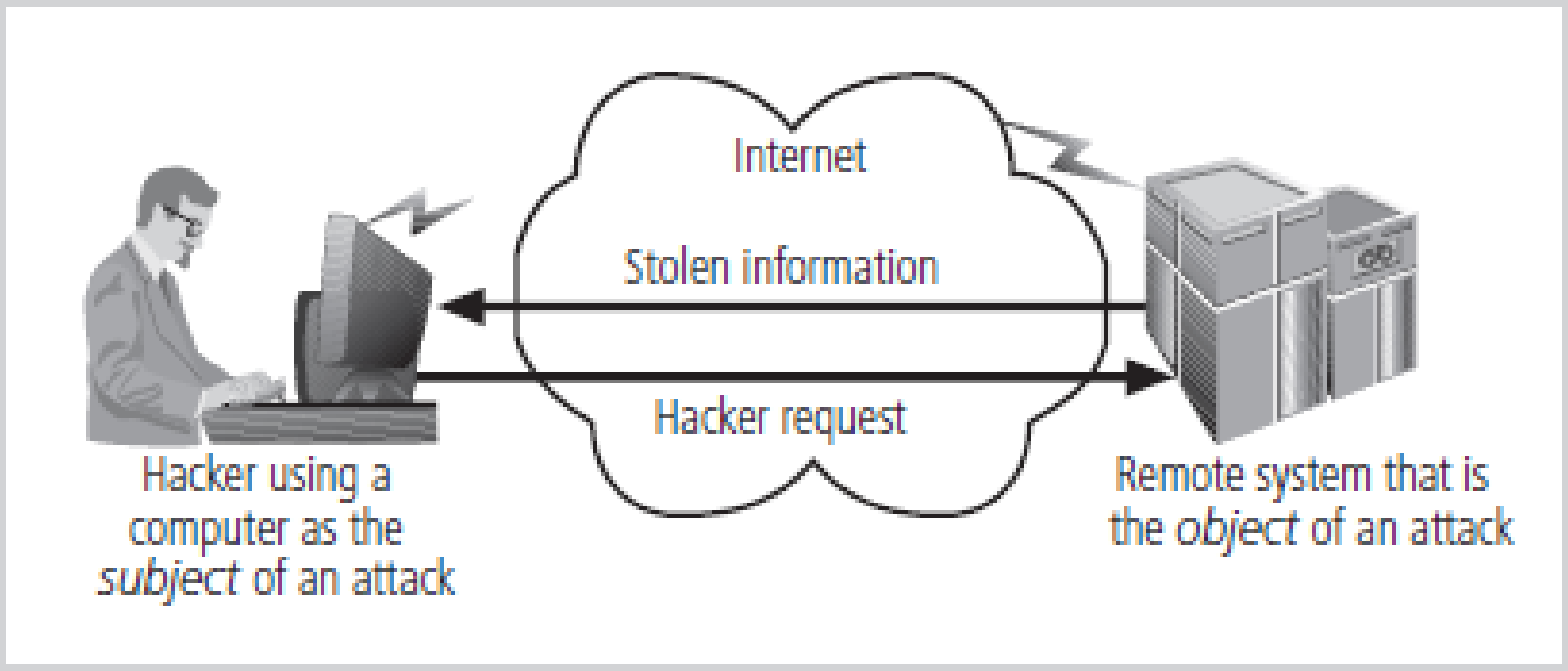

Internet
Stolen information
Hacker request
Hacker using a computer as the *subject* of an attack
Remote system that is the *object* of an attack

Figure Computer as the Subject and Object of an Attack

Loss

Loss: A single instance of an information asset suffering damage or destruction, unintended or unauthorized modification or disclosure, or denial of use.

- When an organization’s information is stolen, it has suffered a loss.

Example:

- **Target**: A bank contains money.
- **Threat**: There are individuals who want, or need additional money.
- **Vulnerability**: The bank uses software that has a security flaw.
- **Exposure**: 20% of the bank's assets are affected by this flaw.
- **Exploit**: By running a small snippet of code (malware), the software can be accessed illegally.
- **Threat** Agent: There are hackers who have learned how to use this malware to control the bank's software.
- **Exploitation**: The hackers access the software using the malware and steal money.
- **Impact**: The bank loses monetary assets, reputation, and future business.
- **Risk**: The likelihood that a hacker will exploit the bank's software vulnerability and impact the bank's reputation and monetary resources.

Critical Characteristics of Information

The value of information comes from the characteristics it possesses:

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

Critical Characteristics of Information

The value of information comes from the **characteristics** it possesses.

- **Availability** – Enables users who need to access information to do so without interference or obstruction and in the required format. The information is said to be available to an authorized user when and where needed and in the correct format.
- **Accuracy** – Free from mistake or error and having the value that the end user expects. If information contains a value different from the user's expectations due to the intentional or unintentional modification of its content, it is no longer accurate.
- **Authenticity** –The quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is the information that was originally created, placed, stored, or transferred.
- **Confidentiality** – The quality or state of preventing disclosure or exposure to unauthorized individuals or systems.

Critical Characteristics of Information – Cont’d

- **Integrity** – The quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state.
- **Utility** – The quality or state of having value for some purpose or end. Information has value when it serves a particular purpose. This means that if information is available, but not in a format meaningful to the end user, it is not useful.
- **Possession** – The quality or state of having ownership or control of some object or item. Information is said to be in possession if one obtains it, independent of format or other characteristic. While a breach of confidentiality always results in a breach of possession, a breach of possession does not always result in a breach of confidentiality.

Balancing Information Security and Access

- Impossible to obtain perfect security
- Process, not an absolute
- Security should be considered balance between protection and availability
- Must allow reasonable access, yet protect against threats

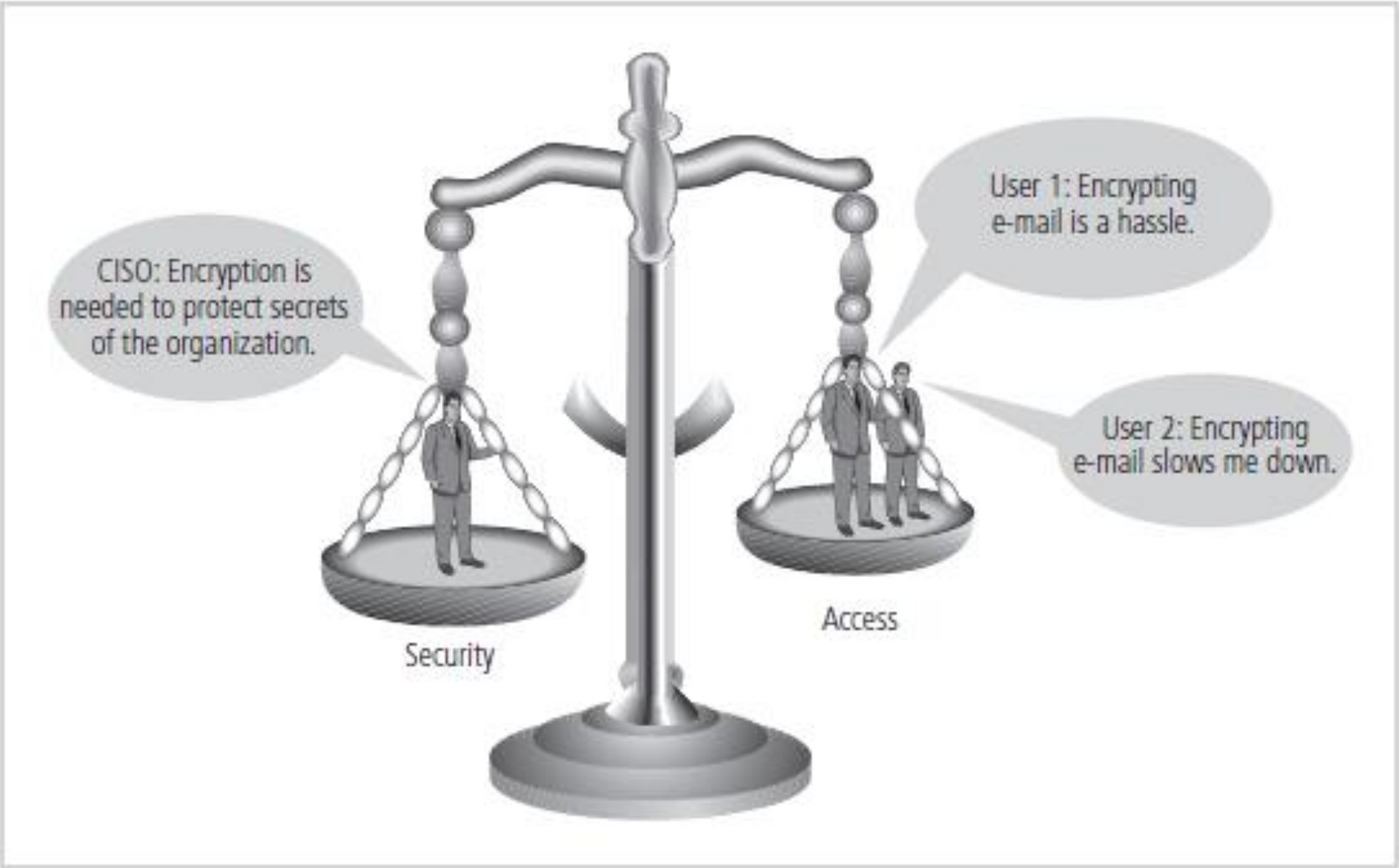

CISO: Encryption is needed to protect secrets of the organization.
User 1: Encrypting e-mail is a hassle.
User 2: Encrypting e-mail slows me down.
Security
Access

Figure 1-8 Balancing Information Security and Access

Bottom-Up Approach

- Security can begin as a grass-roots effort when systems administrators attempt to improve the security of their systems. This is referred to as the **bottom-up approach**.
- The key advantage of the bottom-up approach is the technical expertise of the individual administrators.
- Unfortunately, this approach seldom works, as it lacks a number of critical features, such as participant support and organizational staying power.

Approaches to Information Security Implementation: **Bottom-Up Approach**

- Grassroots effort -systems administrators drive
- Key advantage: technical expertise of individual administrators
- Seldom works
- Lacks number of critical features:
  - Participant support
  - Organizational staying power

Top-down Approach to Security Implementation

- An alternative approach, which has a higher probability of success, is called the **top-down approach**. The project is initiated by upper management who issue policy, procedures, and processes; dictate the goals and expected outcomes of the project; and determine who is accountable for each of the required actions.
- The top-down approach has strong upper-management support, a dedicated champion, dedicated funding, clear planning, and the opportunity to influence organizational culture.
- The most successful top-down approach also involves a formal development strategy referred to as a systems development life cycle.

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
- Most successful
- Involves formal development strategy
- Systems development life cycle

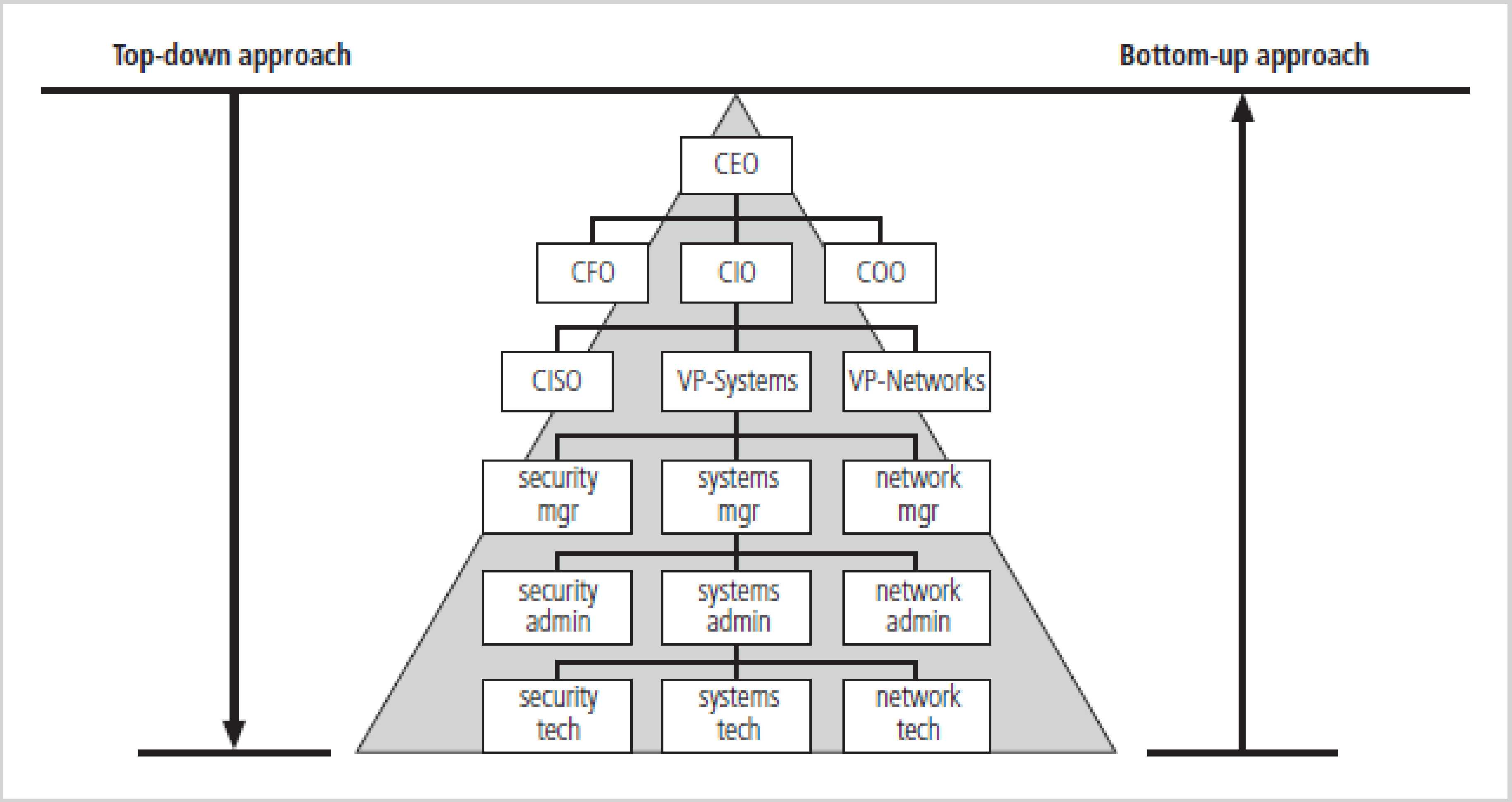


Figure 1-9 Approaches to Information Security Implementation

The Systems Development Life Cycle

- Information security must be managed in a manner similar to any other major system implemented in the organization.
- The best approach for implementing an information security system in an organization with little or no formal security in place is to use a variation of the Systems Development Life Cycle (SDLC): the Security Systems Development Life Cycle (SecSDLC).
- The SDLC is a methodology for the design and implementation of an information system in an organization.
- A methodology is a formal approach to solving a problem based on a structured sequence of procedures.
- Using a methodology ensures a rigorous process and avoids missing those steps that can lead to compromising the end goal.
- The goal is creating a comprehensive security posture.

The Systems Development Life Cycle – Cont’d

- Systems Development Life Cycle (SDLC):
  - Methodology for design and implementation of information system
- Methodology:
  - Formal approach to problem solving
  - Based on structured sequence of procedures
- Using a methodology:
  - Ensures a rigorous process
  - Increases probability of success
- Traditional SDLC consists of six general phases

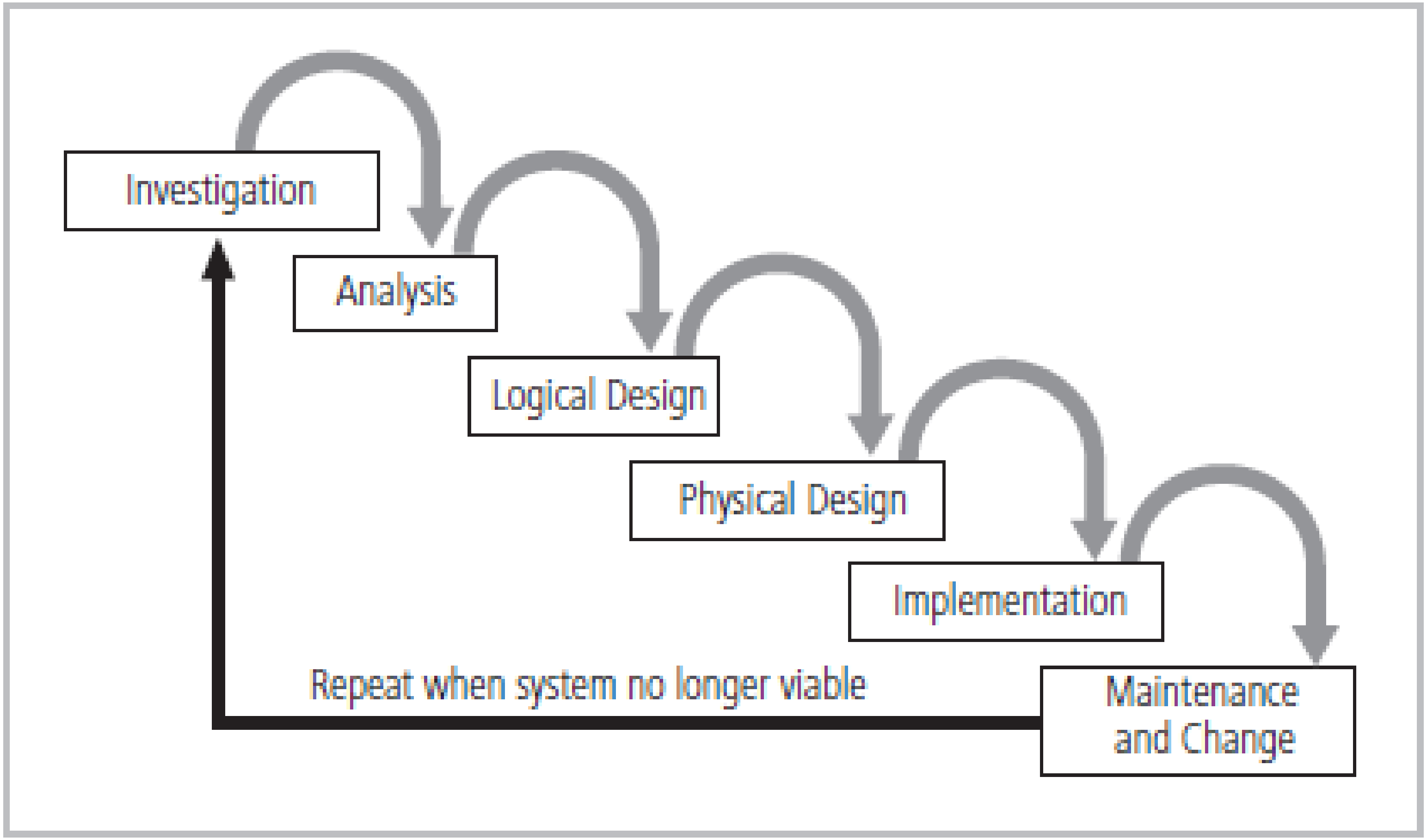


Figure 1-10 SDLC Waterfall Methodology

Investigation

- What problem is the system being developed to solve?
- Objectives, constraints, and scope of project specified
- Preliminary cost-benefit analysis developed
- At end
    - Feasibility analysis performed
        - Assess economic, technical, and behavioural feasibilities

Analysis

- Consists of assessments of:
  - The organization
  - Current systems
  - Capability to support proposed systems
- Determine what new system is expected to do
- Determine how it will interact with existing systems
- Ends with documentation

Logical Design

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

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

Implementation

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

Maintenance and Change

- Longest and most expensive phase
- Tasks necessary to support and modify system
  - Last for product useful life
- Life cycle continues
  - Process begins again from the investigation phase
- When current system can no longer support the organization’s mission, a new project is implemented

The Security Systems Development Life Cycle

- The same phases used in traditional SDLC
- Need to adapted to support implementation of an IS project
- Identify specific threats and creating controls to counter them
- SecSDLC is a coherent program not series of random, seemingly unconnected actions

Investigation

- Identifies process, outcomes, goals, and constraints of the project
- Begins with Enterprise Information Security Policy (EISP)
- Organizational feasibility analysis is performed

Analysis

- Documents from investigation phase are studied
- Analysis of existing security policies or programs
- Analysis of documented current threats and associated controls
- Analysis of relevant legal issues that could impact design of the security solution
- Risk management task begins

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 be continued or outsourced

Physical Design

- Needed security technology is evaluated
- Alternatives are generated
- Final design is selected
- At end of phase, feasibility study determines readiness of organization for project

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, repairing damage and restoring 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 and the Organization

- Wide range of professionals required to support a diverse information security program
- Senior management is key component
- Additional administrative support and technical expertise are 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 required technical and nontechnical 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

Communities of Interest

- Group of individuals united by similar interests/values within an organization
  - Information security management and professionals
  - Information technology management and professionals
  - Organizational management and professionals

Information Security: Is it an Art or a Science?

- Implementation of information security often described as combination of art and science
- “Security artisan” idea: based on the way individuals perceive systems technologists since computers became commonplace

Security as Art

- No hard and fast rules nor many universally accepted complete solutions
- No manual for implementing security through entire system

Security as Science

- Dealing with technology designed to operate at high levels of performance
- Specific conditions cause virtually all actions that occur in computer systems
- Nearly every fault, security hole, and systems malfunction are a result of interaction of specific hardware and software
- If developers had sufficient time, they could resolve and eliminate faults

Security as a Social Science

- Social science examines the behaviour of individuals interacting with systems
- Security begins and ends with the people that interact with the system
- Security administrators can greatly reduce levels of risk caused by end users, and create more acceptable and supportable security profiles