WMSU

IT 143
INFORMATION ASSURANCE AND SECURITY

Principles of Information Security
Chapter 1: Introduction to Information Security

CEED JENNELLE B. LORENZO

College of Computing Studies
Department of Information Technology

Learning and Objectives

- What is information security
- History of computer security and how it evolved into information security
- Concepts of information security
- Phases of the security systems development life cycle
- Information security roles of professionals within an organization

Introduction

- 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

History of Information Security

Began immediately following development first mainframes

- Developed for code-breaking computations
- During World War II
- Multiple levels of security were implemented

- Physical controls
- Rudimentary
  - Defending against physical theft, espionage, and sabotage

1960s

Original communication by mailing tapes

- Advanced Research Project Agency (ARPA)
  - Examined feasibility of redundant networked communications
- Larry Roberts developed ARPANET from its inception
- ARPANET is predecessor to the Internet

1970s and 80s

- ARPANET grew in popularity
- Potential for misuse grew
- Fundamental problems with ARPANET security
  - Individual remote sites were not secure from unauthorized users
  - Vulnerability of password structure and formats
  - No safety procedures for dial-up connections to ARPANET
  - Non-existent user identification and authorization to system

1970s and 80s (cont'd.)

Rand Report R-609

- Paper that started the study of computer security
- Information Security as we know it began

- 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

MULTICS

Early focus of computer security research

- System called Multiplexed Information and Computing Service (MULTICS)

- First operating system created with security as its primary goal
- Mainframe, time-sharing OS developed in mid-1960s
  - GE, Bell Labs, and MIT
- Late 1970s
  - Microprocessor expanded computing capabilities
  - Mainframe presence reduced
  - Expanded security threats

2000 to Present

- Millions of computer networks communicate
- Many of the communication are unsecured
- Ability to secure a computer's data influenced by the security of every computer to which it is connected
- Growing threat of cyber attacks has increased the need for improved security

What is Security?

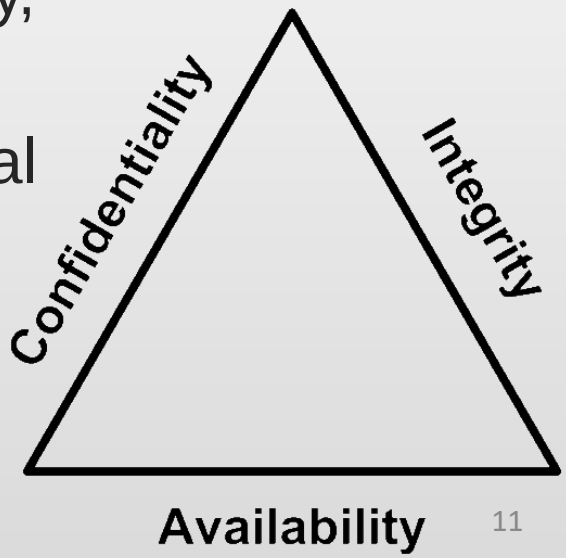
"The quality or state of being secure—to be free from danger"

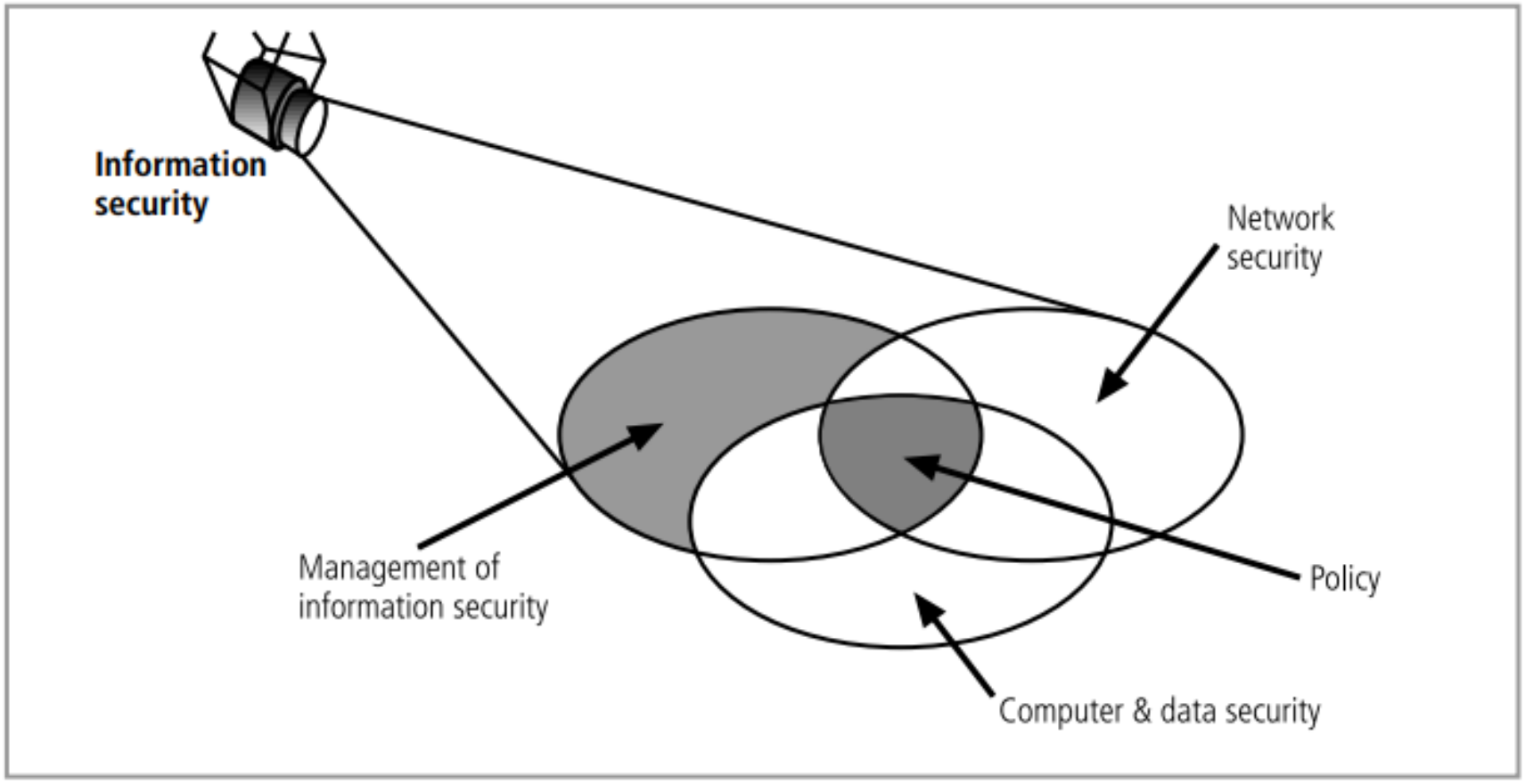
A successful organization should have multiple layers of security in place:

- Physical security
- Personal security
- Operations security
- Communications security
- Network security
- Information security

What is Security? (cont'd.)

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- C.I.A. triangle
  - Was standard based on confidentiality, integrity, and availability
  - Now expanded into list of critical characteristics of information





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**
  - Protected organizational resource
- **Attack**
  - Intentional or unintentional; active or passive; direct or indirect attack

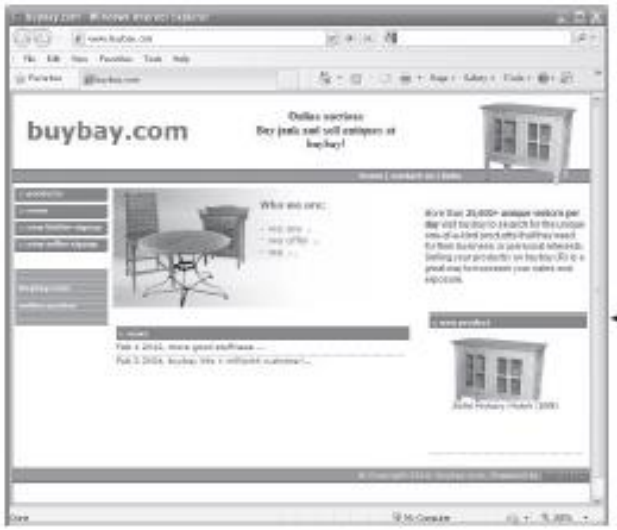
Key Information Security Concepts

- **Control, safeguard, or countermeasure**
  - Security mechanisms, policies or procedures
- **Exploit**
  - Used to compromise a system
- **Exposure**
  - A condition or state of being exposed
- **Loss**
  - Information asset suffering from a damage

Key Information Security Concepts

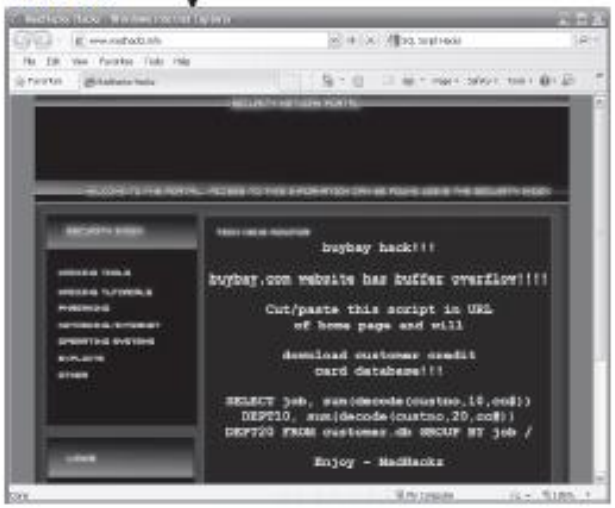
- **Risk**
  - Probability of something unwanted will happen
- **Subjects or objects**
  - Computer as a subject or object of an attack
- **Threat**
  - Entities that present danger to an asset
- **Threat agent**
  - specific instance or a component of a threat
- **Vulnerability**
  - Weakness or fault in a system

Threat: Theft
Threat agent: Ima Hacker



Vulnerability: Buffer overflow in online database Web interface

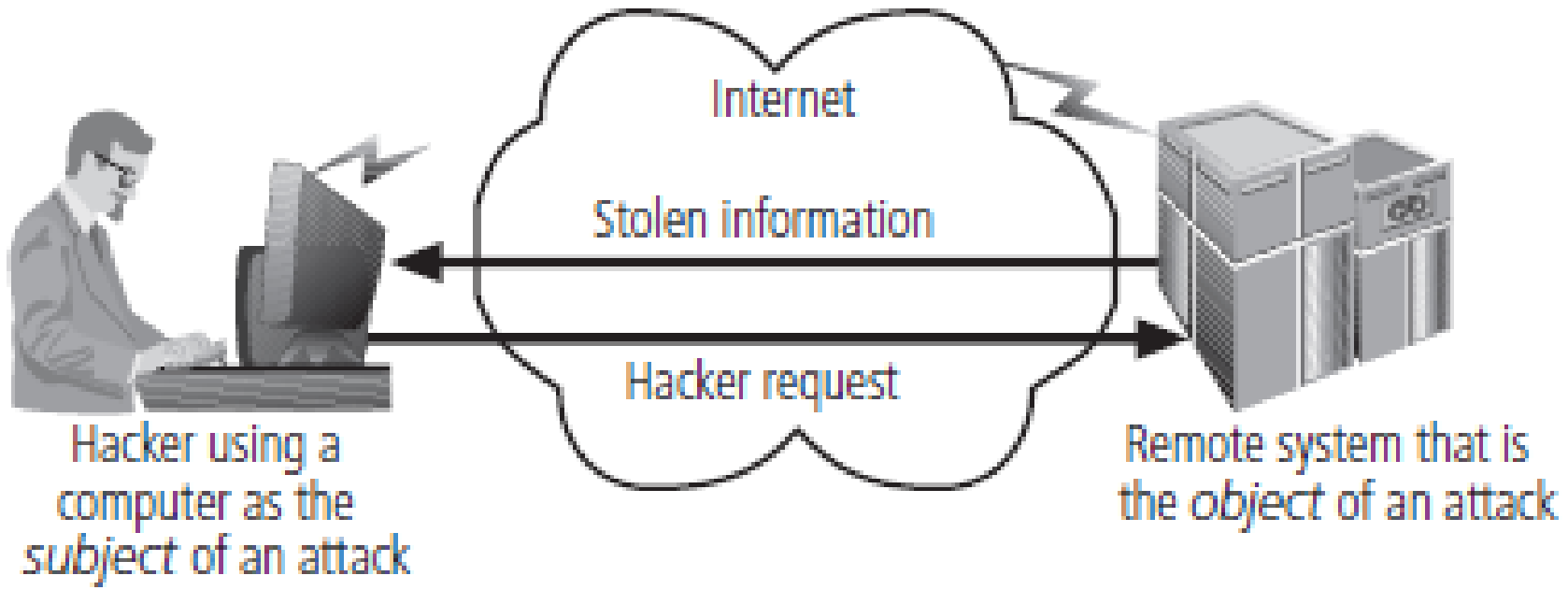
Exploit: Script from MadHackz Web site



Attack: Ima Hacker downloads *exploit* from MadHackz web site, then accesses buybay's Web site and applies script, resulting in **loss:** download of customer data

Asset: buybay's customer database

Information Security Terms



Computer as the subject and Object of an attack

Critical characteristics of Information

- The value of information comes from the characteristics it possesses:
  - Authenticity
  - Confidentiality
  - Availability
  - Accuracy
  - Integrity
  - Utility
  - Possession

Critical characteristics of Information

- **Authenticity**
  - Information is genuine or original
  - Same state in which it was created, placed, stored or transferred
- **Confidentiality**
  - Only those with sufficient privileges may access certain information

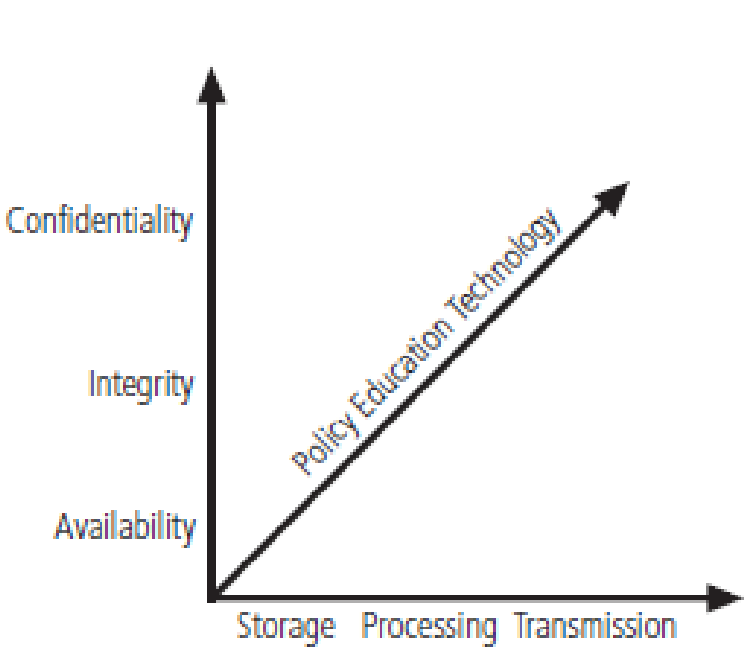
Critical characteristics of Information

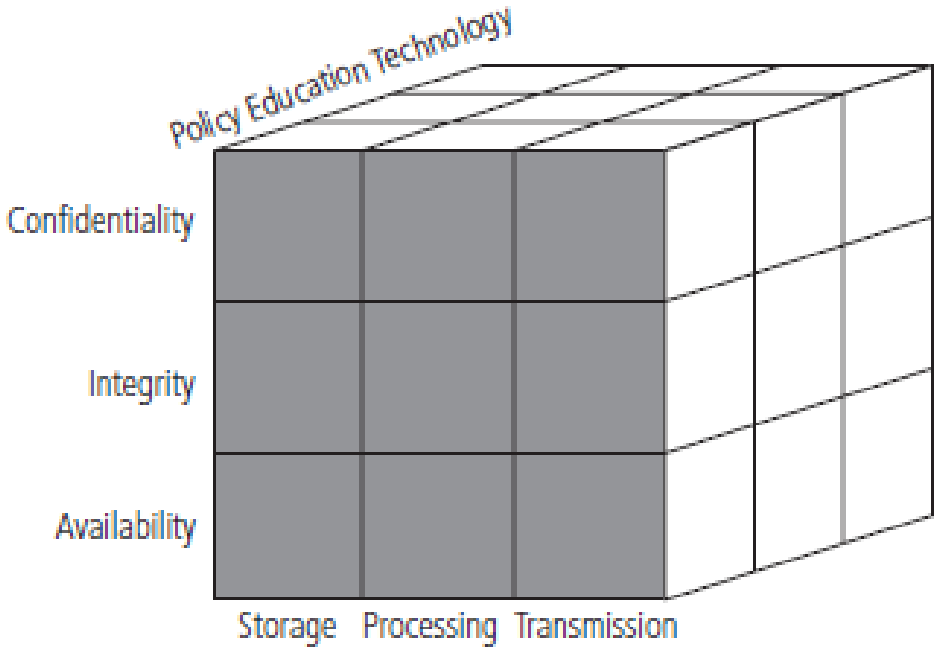
- **Availability**
  - Makes information accessible to authorized users without interference or obstruction.
- **Accuracy**
  - Free from mistakes or errors
  - Has the value that the end user expects
  - If intentionally or unintentionally modified, it is no longer accurate

Critical characteristics of Information

- **Integrity**
  - Quality or state of being whole, complete, and uncorrupted
- **Utility**
  - Information has value when it serves a purpose
- **Possession**
  - Quality or state of ownership or control

CNSS Security Model

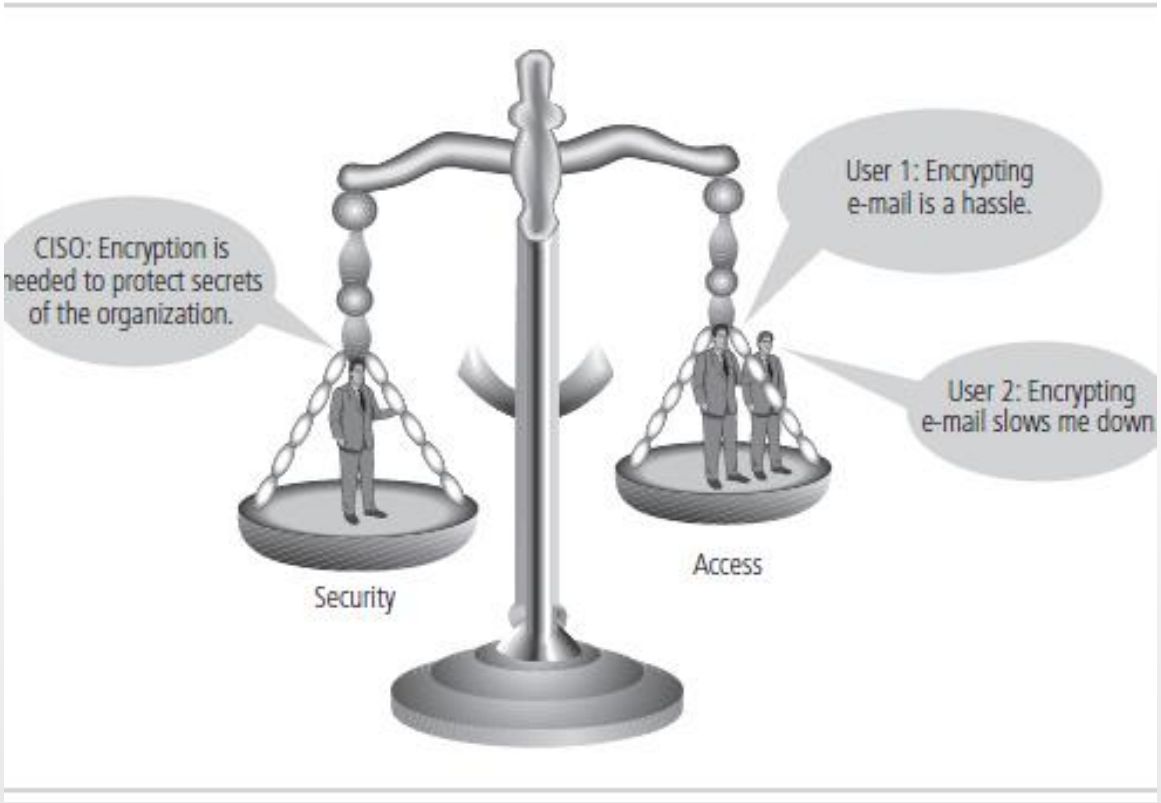




The McCumber Cube

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



Balancing Information Security and Access

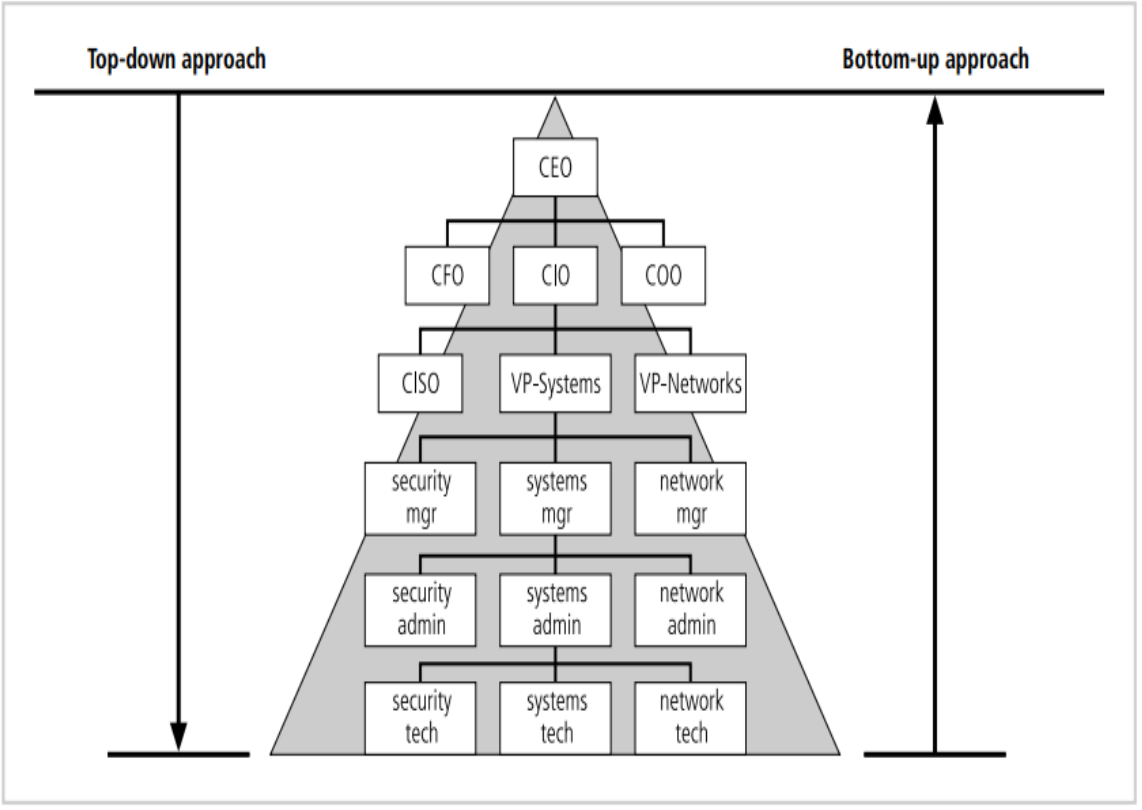
- Impossible to obtain perfect security—it is a process, not an absolute

IS Security Implementation: Bottom-up Approach

- Grassroot effort
  - System administrators
- Advantage: technical expertise of individual administrators
- Lacks number of critical features:
  - Participant support
  - Organizational staying power

IS Security Implementation: Top-Down Approach

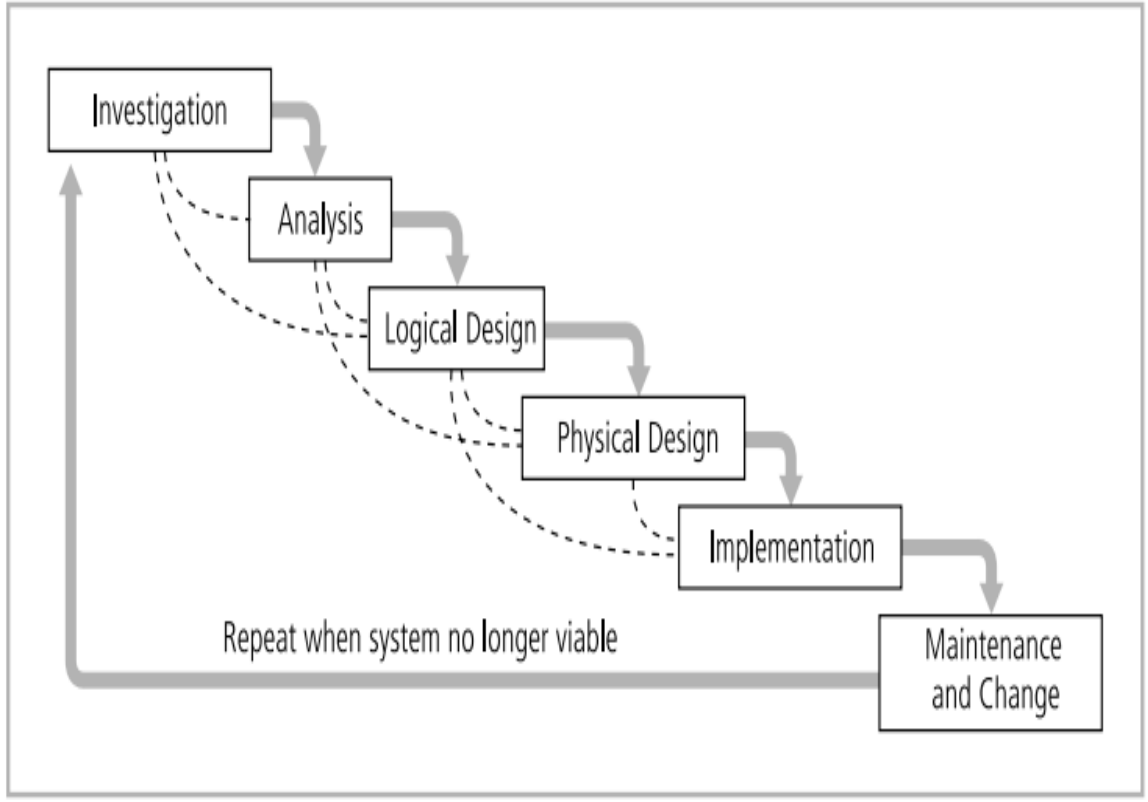
- Initiated by upper management
  - Issue policy, procedures, and processes
  - Dictate goals and expected outcomes of project
  - Determine accountability for each action
- Most successful
- Involves formal development strategy (Systems development life cycle)



Approaches to Information Security Implementation

System Development Life Cycle (SDCLC)

- SDLC: Methodology for design and implementation of information system
- Methodology:
  - Formal approach to problem solving
  - Based on structured sequence of procedures
- Traditional SDLC has 6 general phases



SDLC Waterfall Methodology

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

SDLC Waterfall Methodology: 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

SDLC Waterfall Methodology: 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

SDLC Waterfall Methodology: 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: 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

SDLC Waterfall Methodology: 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 the traditional SDLC
- Implementation of information security
  - Identifying threats
  - Creating specific controls to counter threats
- SecSDLC is a coherent program, not a series of random seemingly unconnected actions

SecSDLC: Investigation

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

SecSDLC: Analysis

- Documents from investigation phase are studied
- Analysis:
  - existing security policies or programs
  - Current threats and associated controls
  - Legal issues
- Risk management task begins

SecSDLC: Logical Design

- Creates and develops blueprints for information security
- Incident response actions planned:
  - Continuity planning
  - Incident response
  - Disaster recovery
- Feasibility analysis – whether the project should be continued or not

SecSDLC: Physical Design

- Evaluates the IS technology needed
- Alternatives are generated
- Final design is selected
- End of the phase:
  - Feasibility study to determine readiness of the project

SecSDLC: 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

SecSDLC: Maintenance and Change

- 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 owners
  - responsible for the security
  - use of a particular set of information
- Data custodian
  - responsible for the storage, maintenance, and protection of the information
- Data users
  - work with the information to perform their daily jobs supporting the mission of the organization

- Each organization has a culture in which communities of interest are united by similar values and share common objectives.
- The three communities in information security are:
  - general management
  - IT management
  - Information security management.

- Information security has been described as both an art and a science, and also comprises many aspects of social science.

References

- Whitman, M. E., & Mattord, H. J.

  (2011). *Principles of information security*. Cengage Learning.