Principles of Information Security, Fourth Edition

Chapter 1

Introduction to Information Security

Do not figure on opponents not attacking; worry about your own lack of preparation.

BOOK OF THE FIVE RINGS

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

The 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

The 1960s

- Original communication by mailing tapes
- Advanced Research Project Agency (ARPA)
  - Examined feasibility of redundant networked communications
- Larry Roberts developed ARPANET from its inception
- Plan
  - Link computers
  - Resource sharing
  - Link 17 Computer Research Centers
  - Cost 3.4M
- ARPANET is predecessor to the Internet

The 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

The 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 MIX
- Several MULTICS key players created UNIX
- Late 1970s
  - Microprocessor expanded computing capabilities
  - Mainframe presence reduced
  - Expanded security threats

The 1990s

- Networks of computers became more common
- Need to interconnect networks grew
- Internet became first manifestation of a global network of networks
- **Initially based on de facto standards**
- In early Internet deployments, security was treated as a low priority

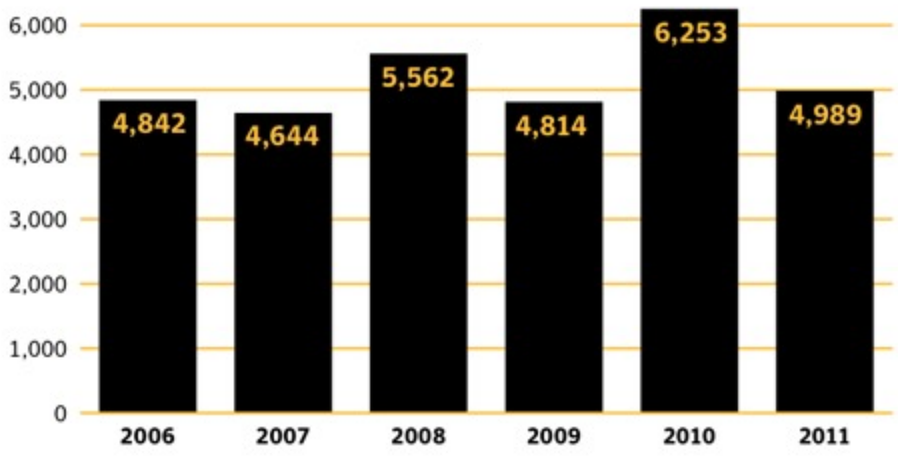
2000 to Present

- Millions of computer networks communicate
- Many of the communication 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

Vulnerabilities

Figure D.1

Total Vulnerabilities Identified, 2006-2011



Source: Symantec.cloud

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
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle
  - Was standard based on confidentiality, integrity, and availability
  - Now expanded into list of critical characteristics of information

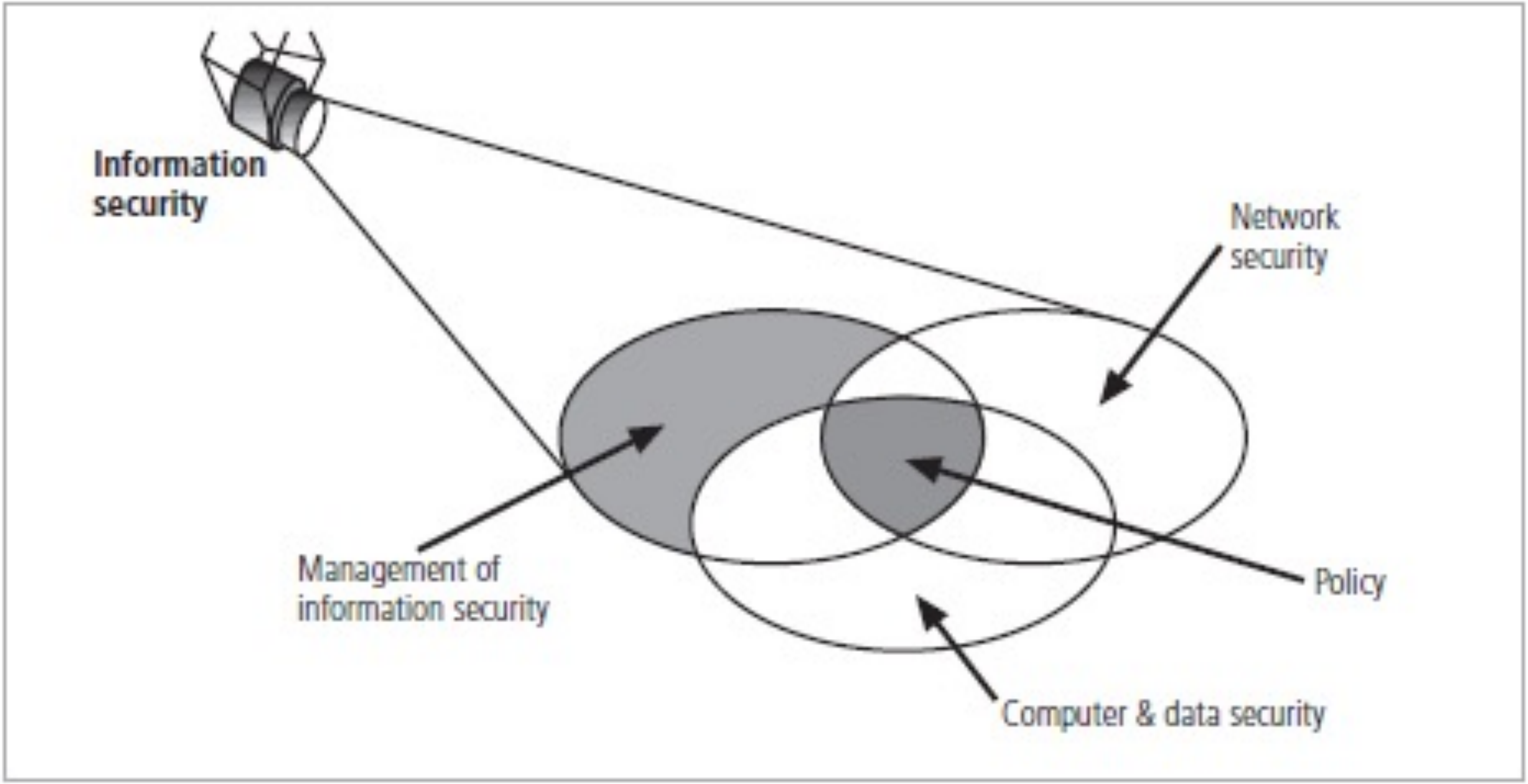


Figure 1-3 Components of Information Security

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 (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

Fi ct of

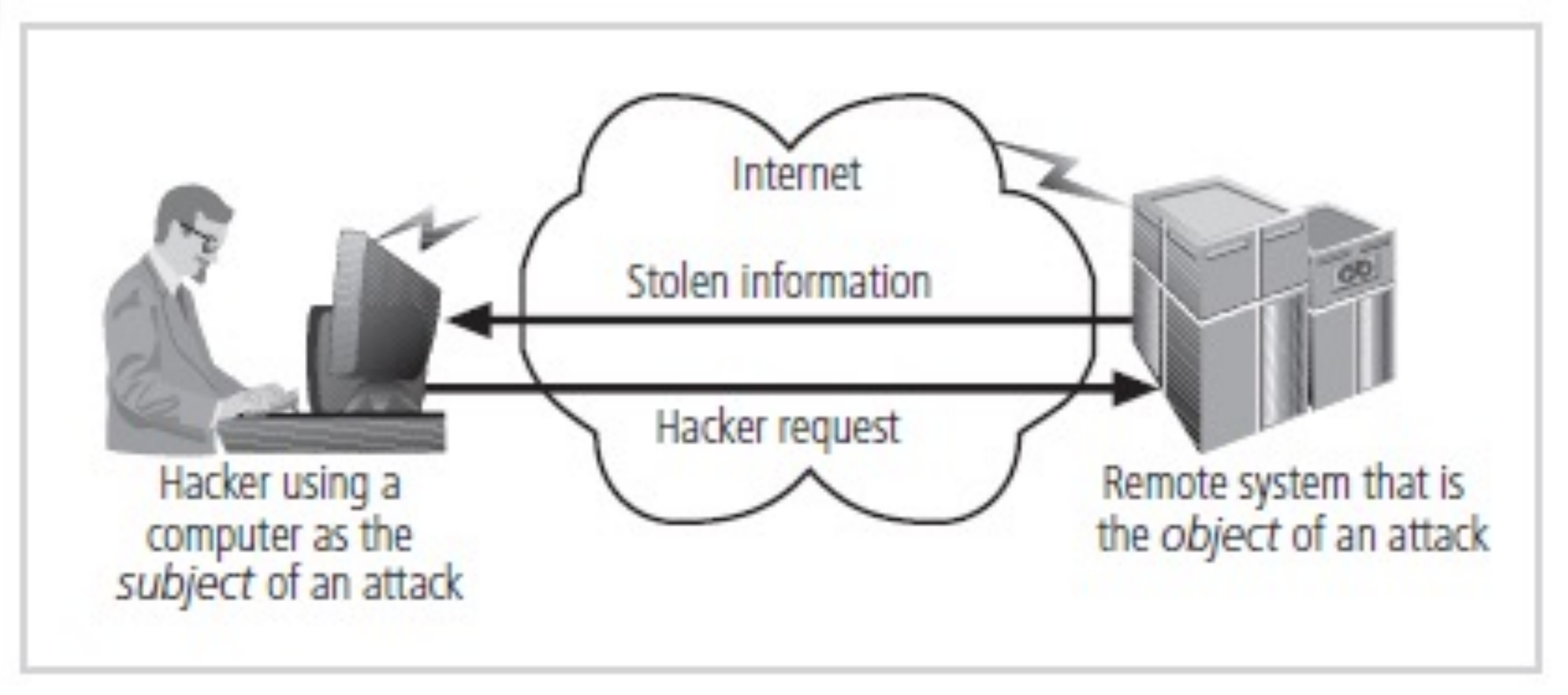

Internet
Stolen information
Hacker request
Hacker using a computer as the *subject* of an attack
Remote system that is the *object* of an attack

Figure 1-5 Computer as the Subject and Object of an Attack

Critical Characteristics of Information

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

CNSS Security Model

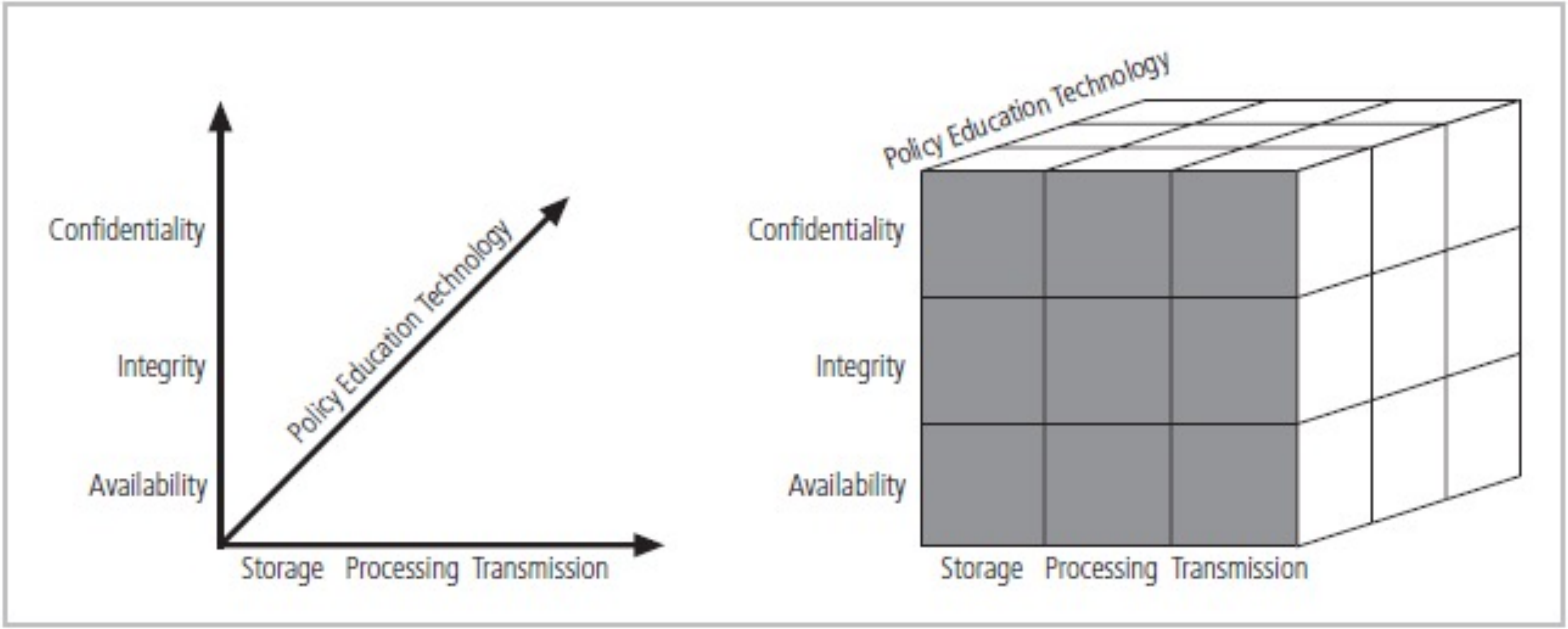


Figure 1-6 The McCumber Cube

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

F

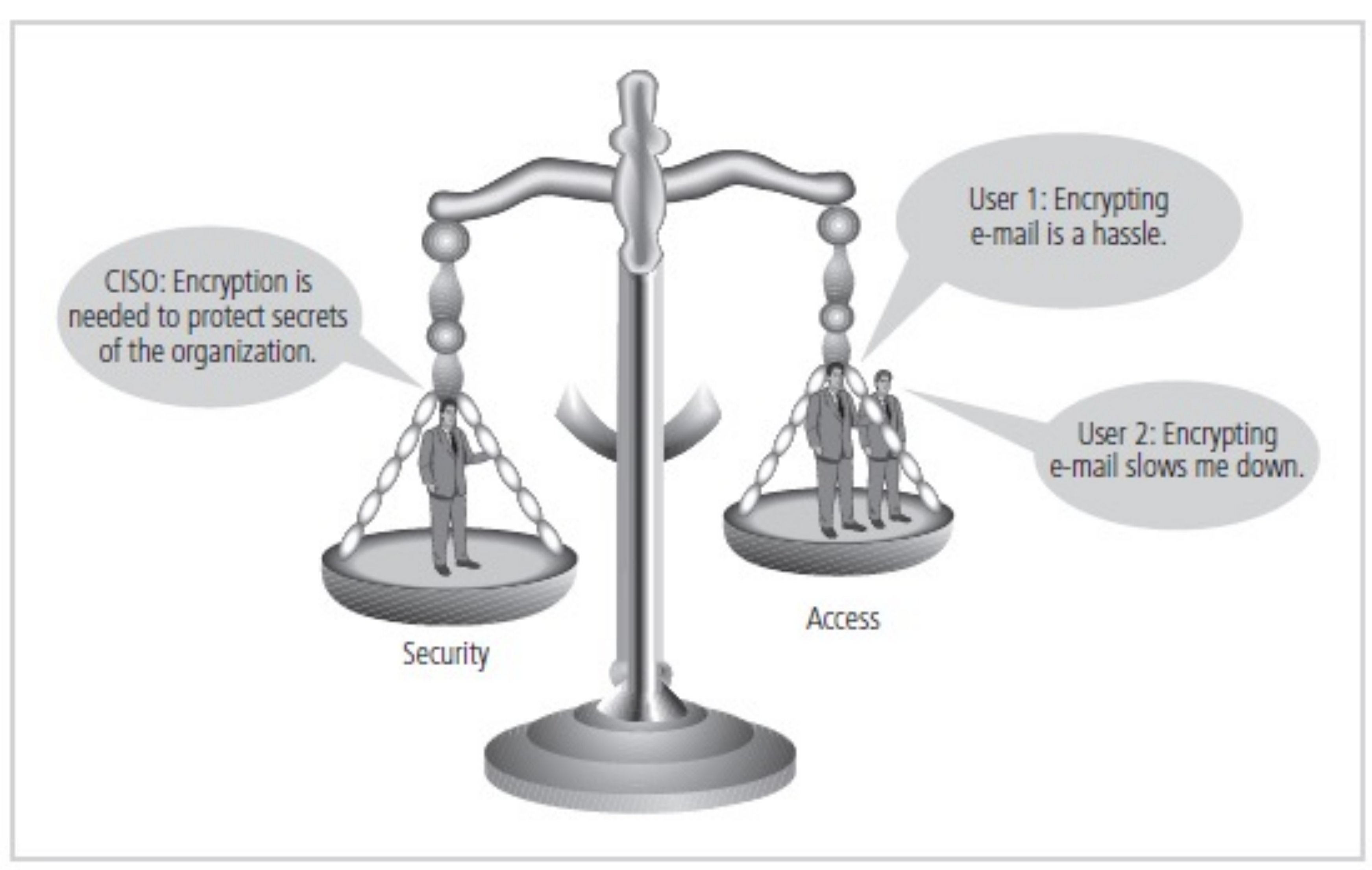

CISO: Encryption is needed to protect secrets of the organization.
User 1: Encrypting e-mail is a hassle.
User 2: Encrypting e-mail slows me down.
Security
Access

Figure 1-8 Balancing Information Security and Access

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

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

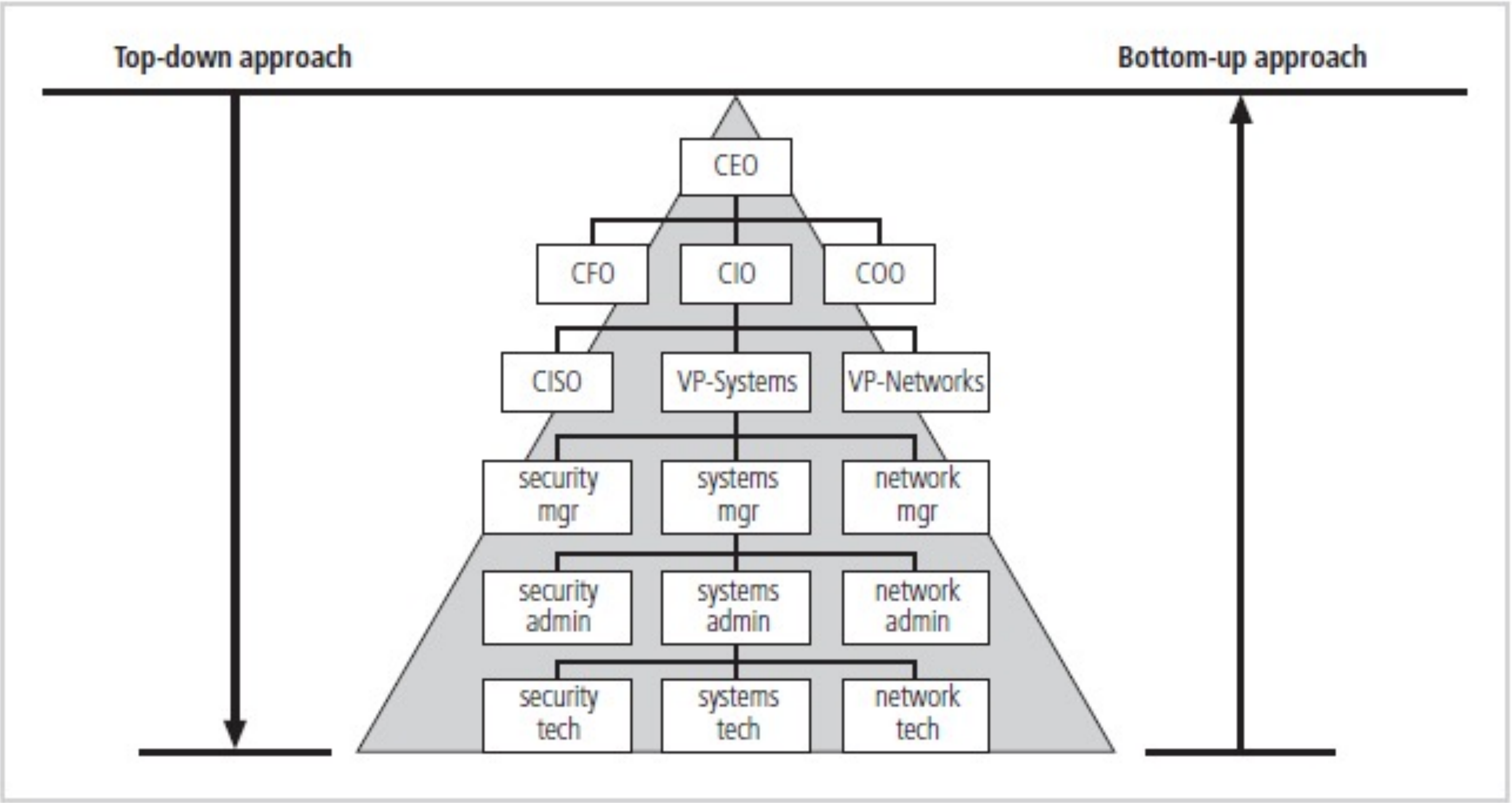


Figure 1-9 Approaches to Information Security Implementation

The Systems Development Life Cycle

- 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

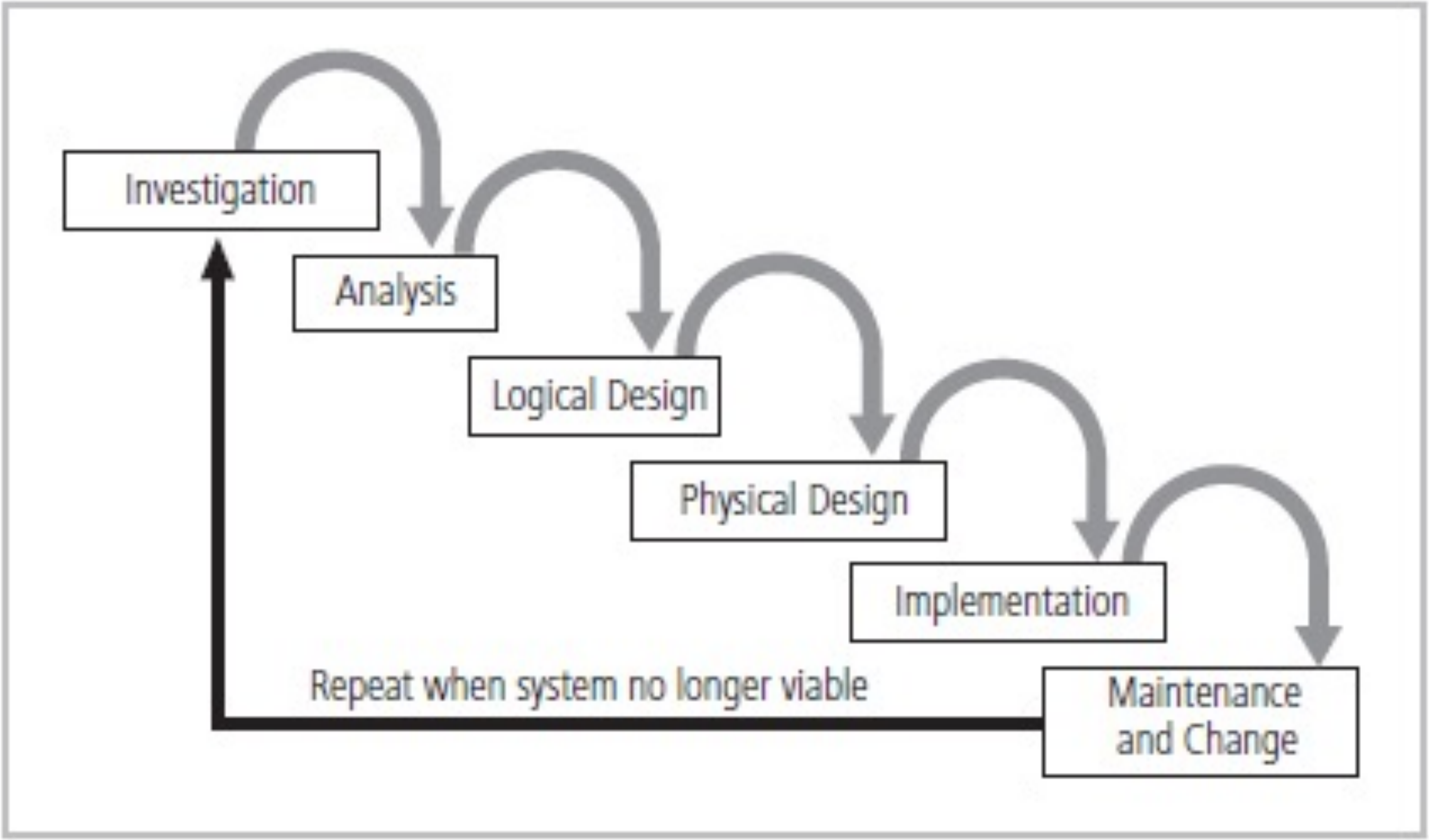


Figure 1-10 SDLC Waterfall Methodology

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