COURSE TECHNOLOGY
CENGAGE Learning™

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

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

The 1970s and 80s

- ARPANET (Advanced Research Project Agency)

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
  - Nonexistent user identification and authorization to system
- Late 1970s: microprocessor expanded computing capabilities and security threats

The 1970s and 80s (cont'd.)

- 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

MULTICS

- Early focus of computer security research was a 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 by General Electric (GE), Bell Labs, and Massachusetts Institute of Technology (MIT)
- Several MULTICS key players created UNIX
- Primary purpose of UNIX was text processing

The 1990s

- Networks of computers became more common; so too did the need to interconnect networks
- 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

- 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
- 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
- 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

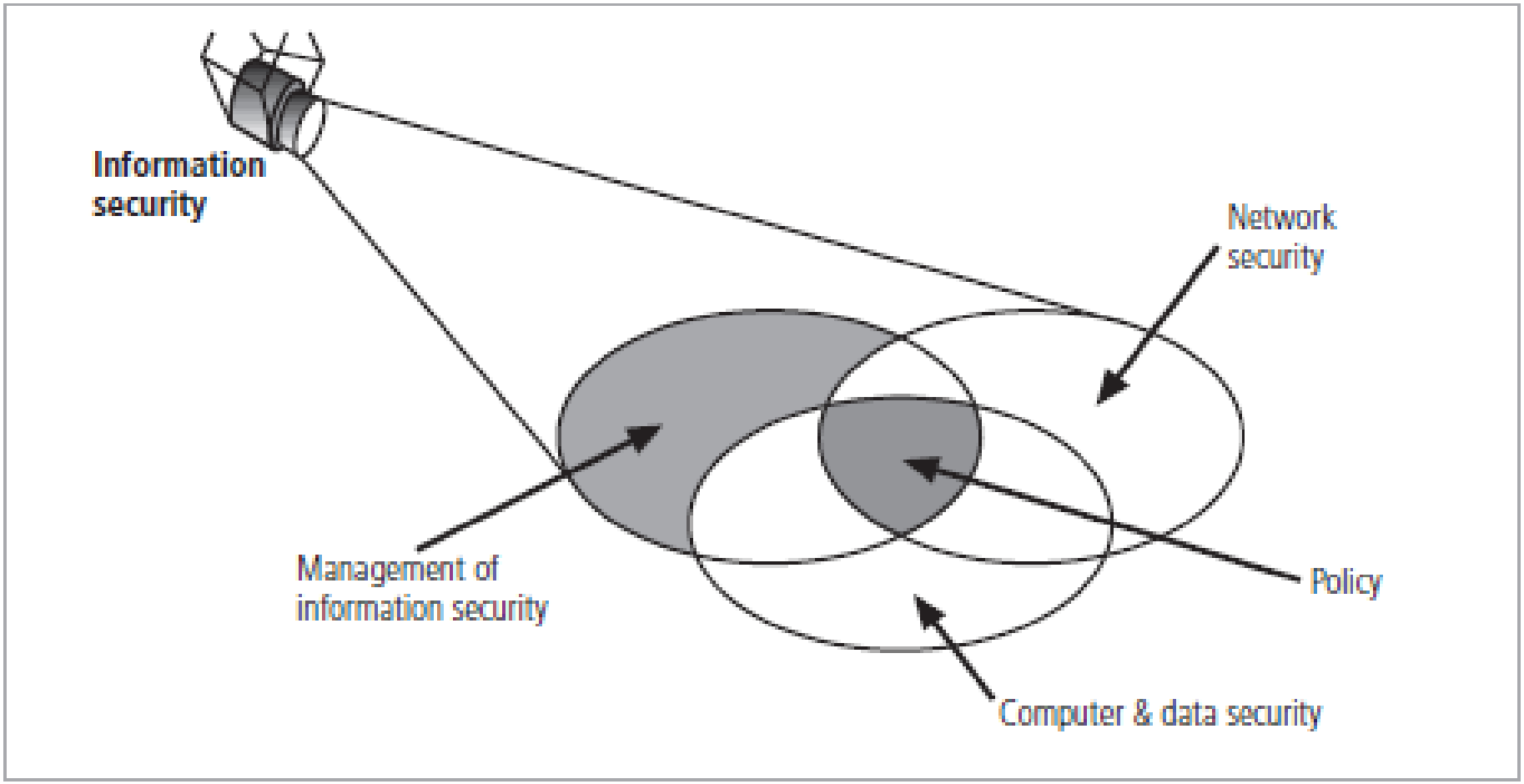

Figure 1-3 Components of Information Security

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

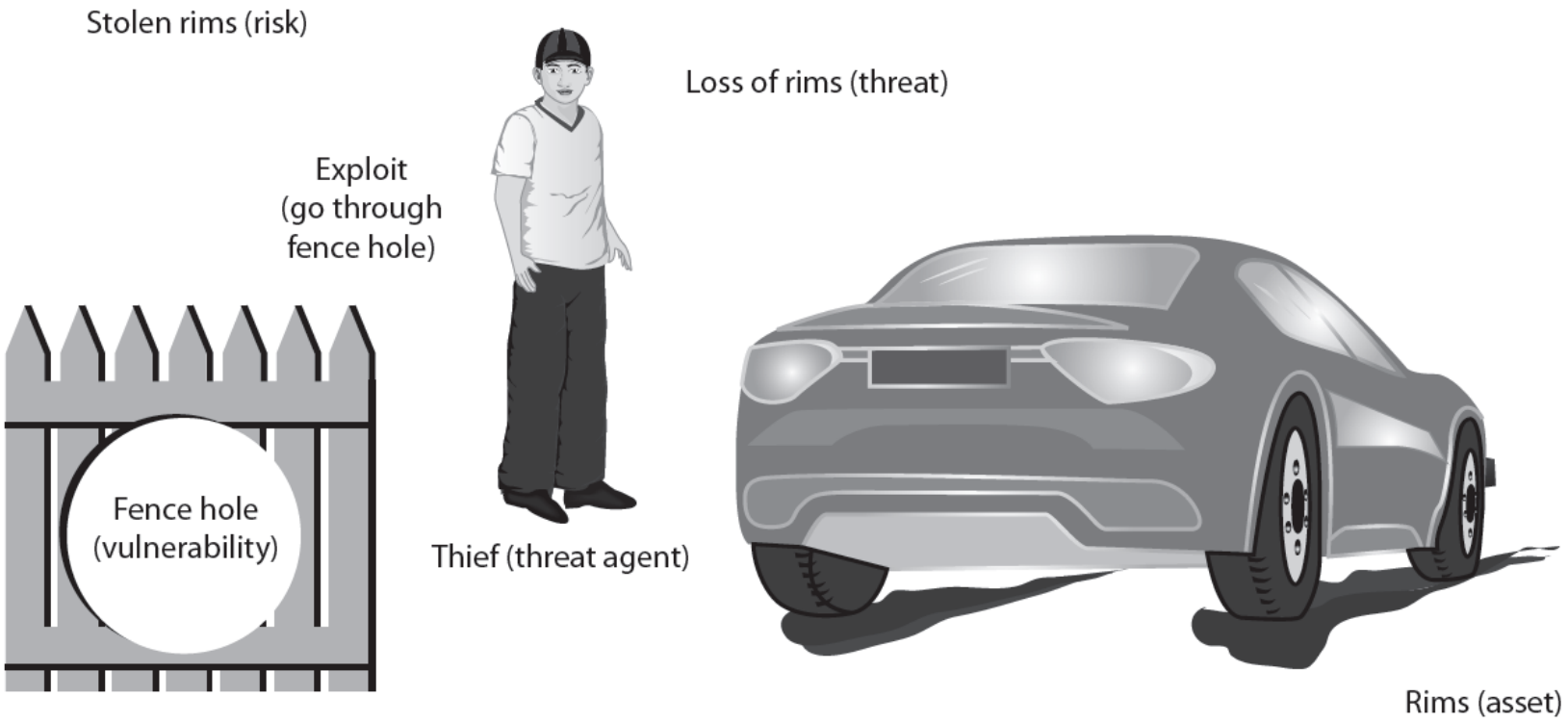

Figure 1-4 Information security components analogy

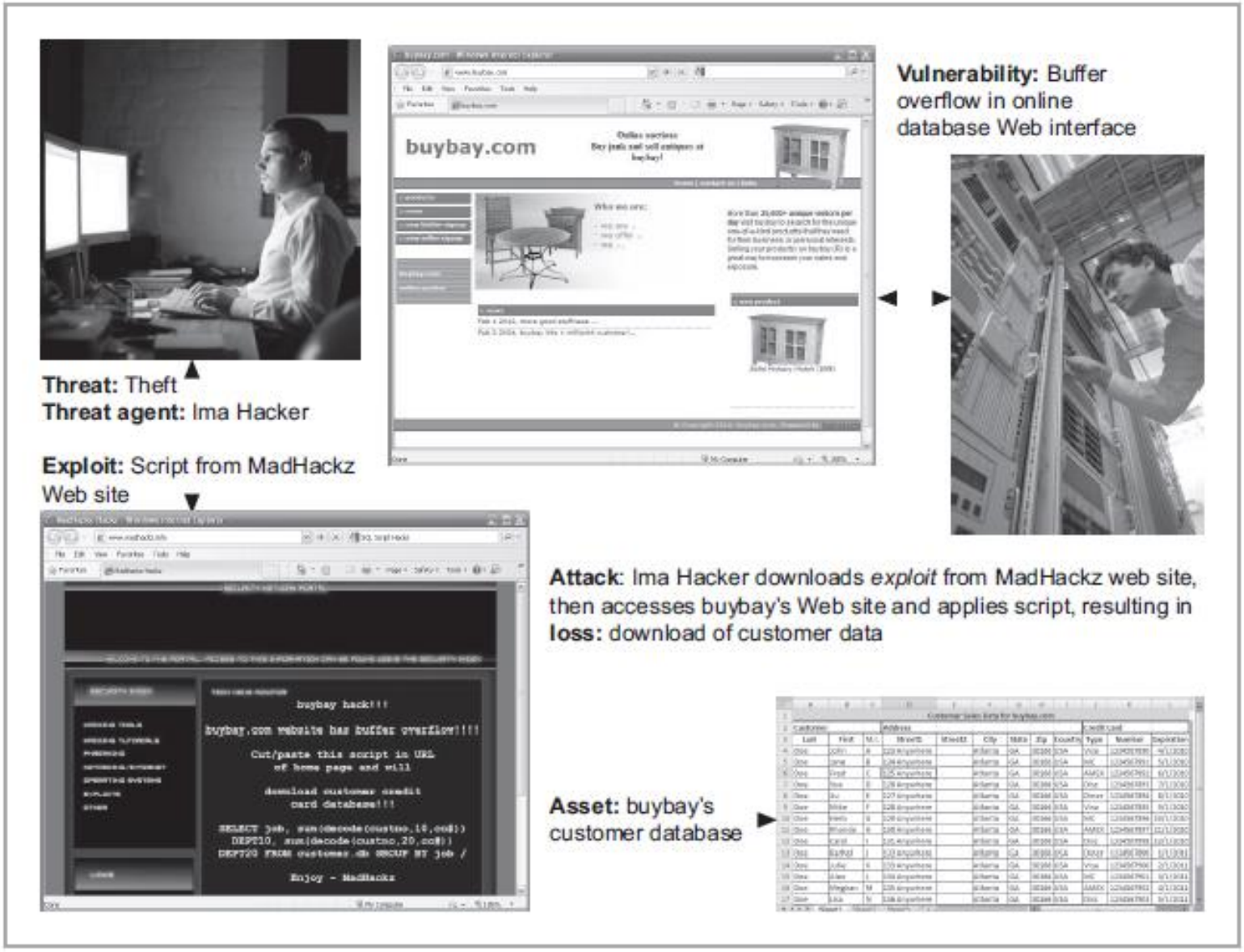

Figure 1-4 Information Security Terms

Critical Characteristics of Information

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

CNSS Security Model

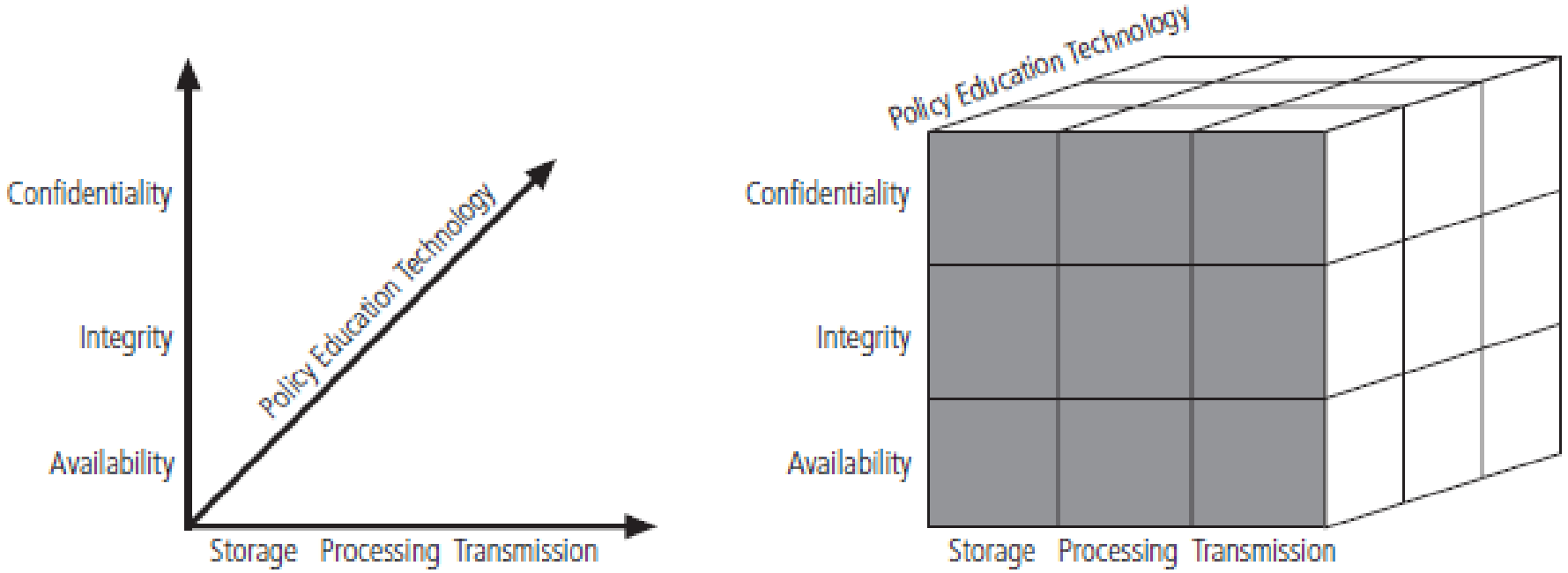

Figure 1-6 The McCumber Cube

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—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

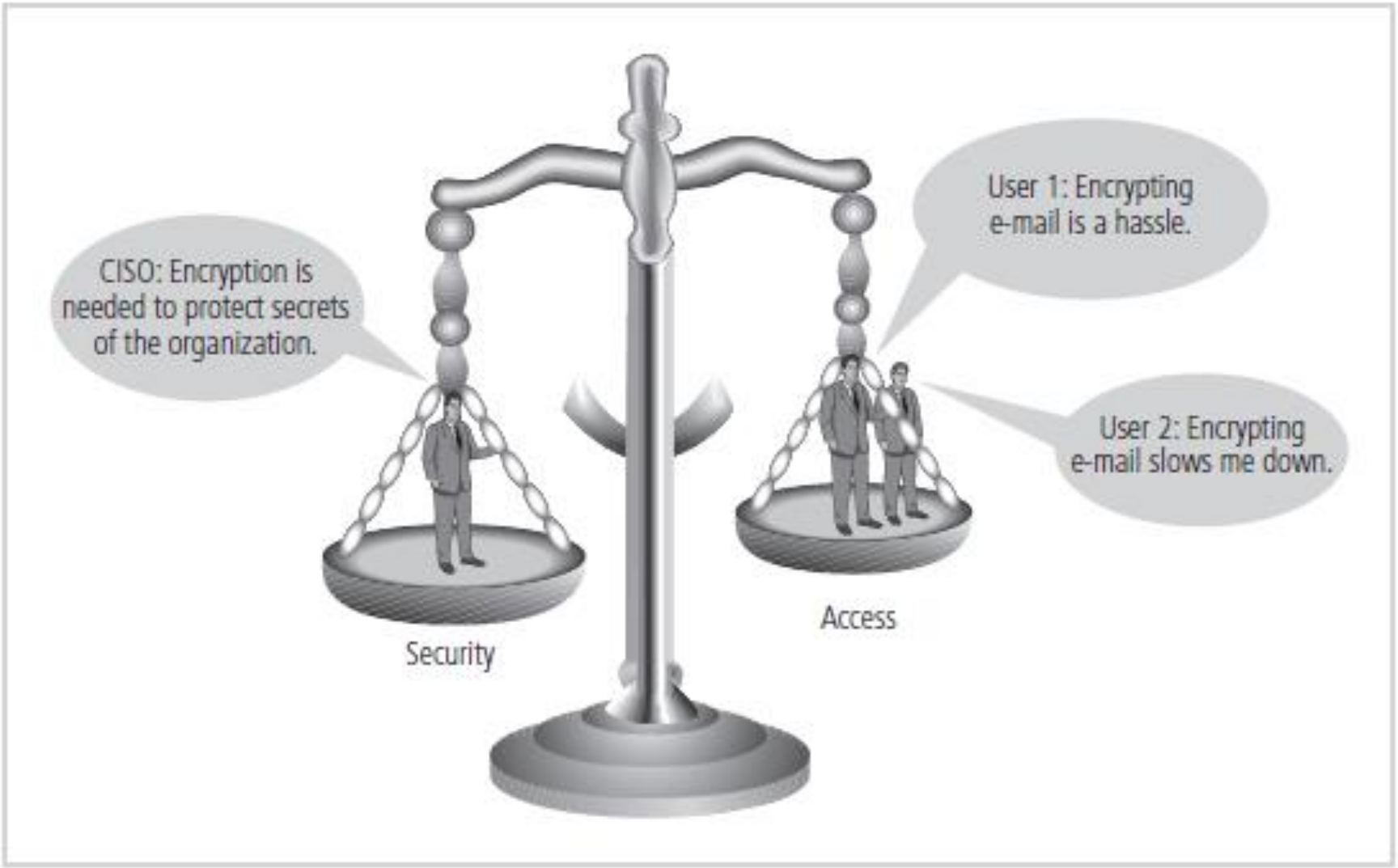

Figure 1-8 Balancing Information Security and Access

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: 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

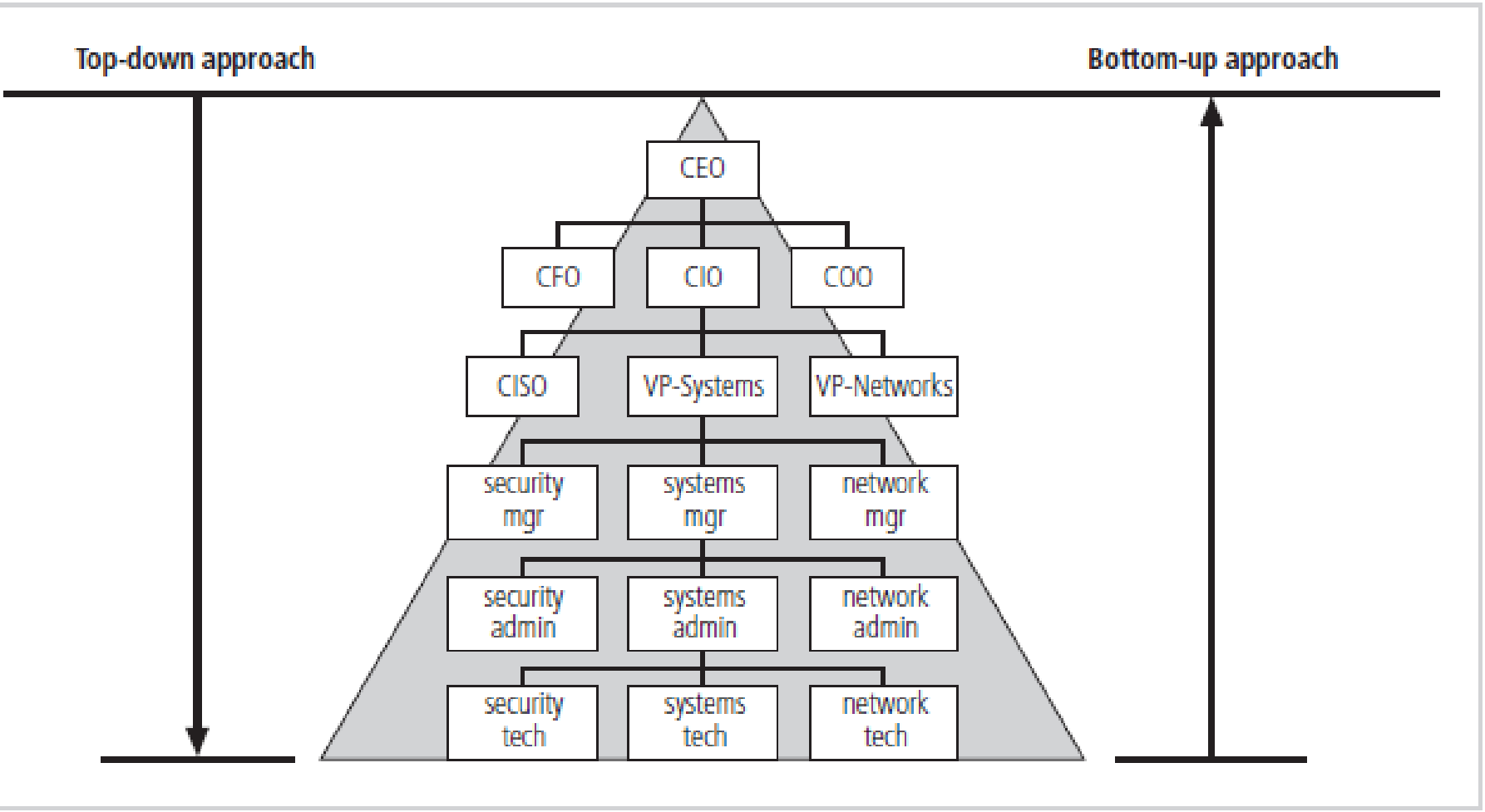

Figure 1-9 Approaches to Information Security Implementation

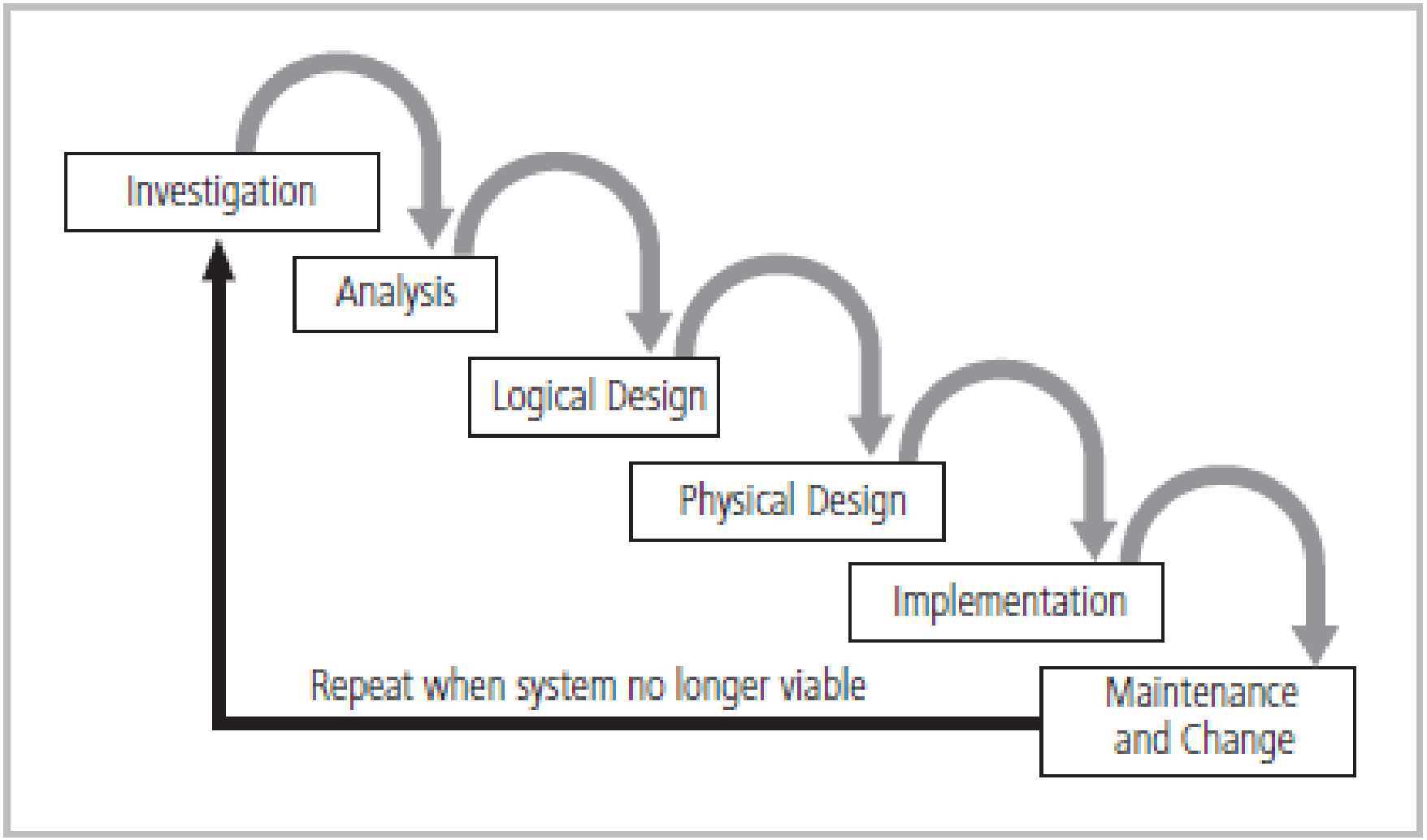

Figure 1-10 SDLC Waterfall Methodology

The Security Systems Development Life Cycle

- The same phases used in traditional SDLC may be adapted to support specialized implementation of an IS project
- Identification of specific threats and creating controls to counter them
- SecSDLC is a coherent program rather than a 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, along with documented current threats and associated controls
- Includes 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, and 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

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