Principles of Information Security

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

Learning Objectives

- Upon completion of this material, you should be able to:
  - Define information security
  - Define key terms and critical concepts of information security
  - Enumerate the phases of the security systems development life cycle
  - Describe the 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)

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

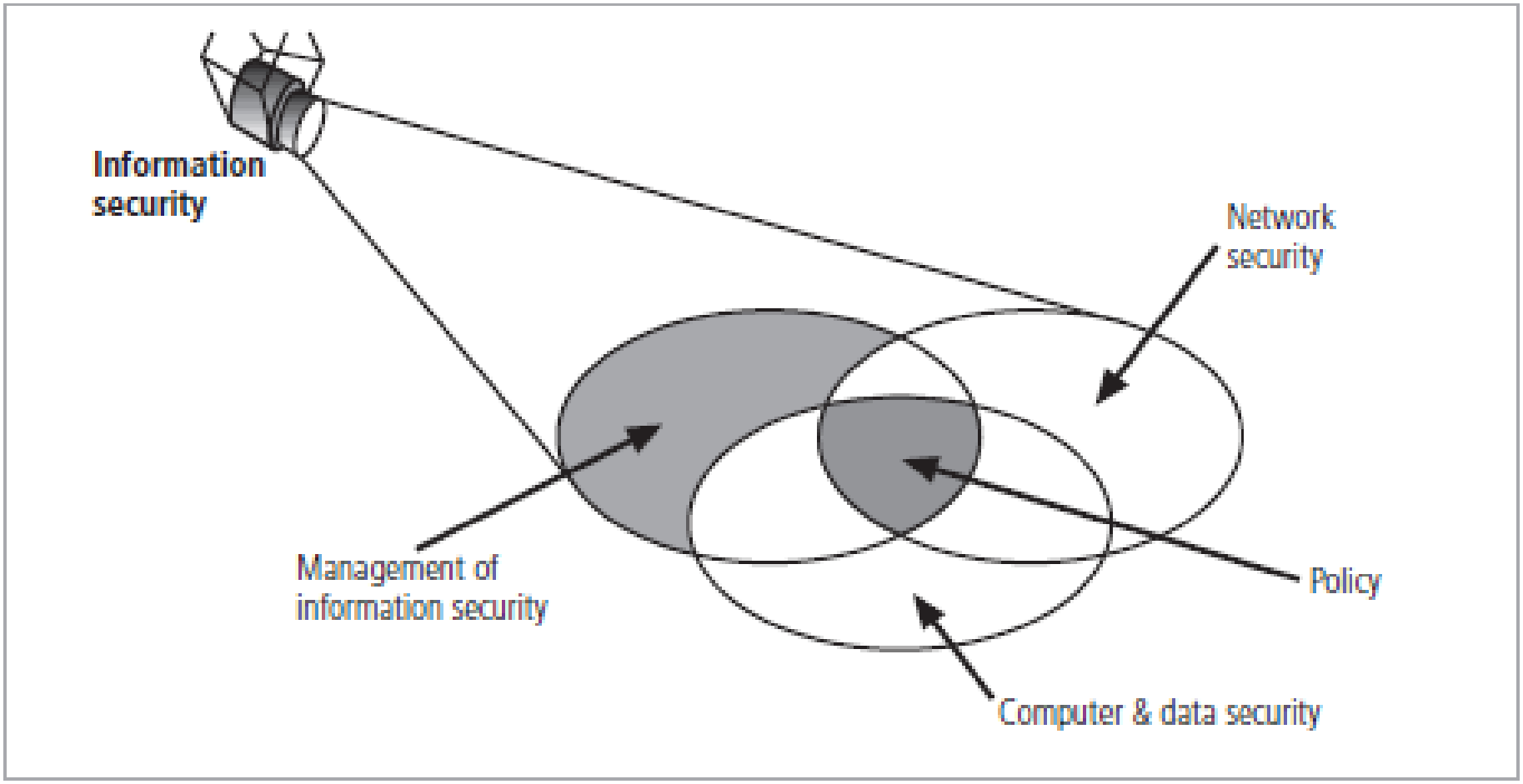
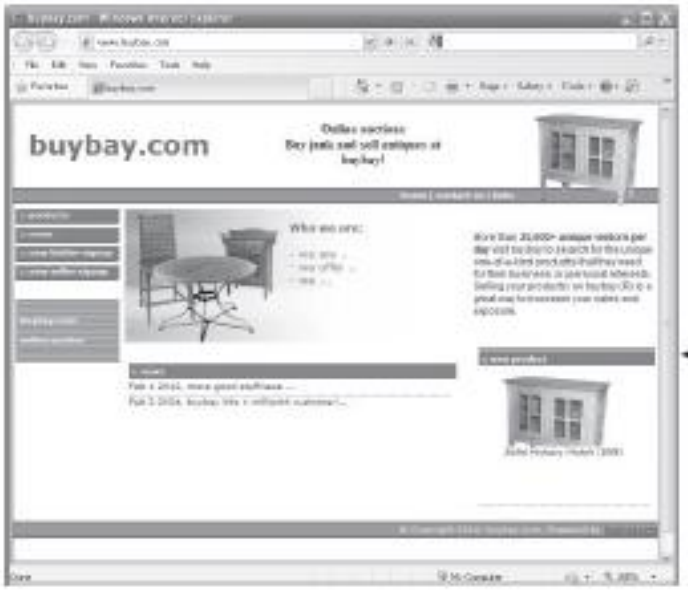


Figure 1-3 Components of Information Security

Key Information Security Concepts

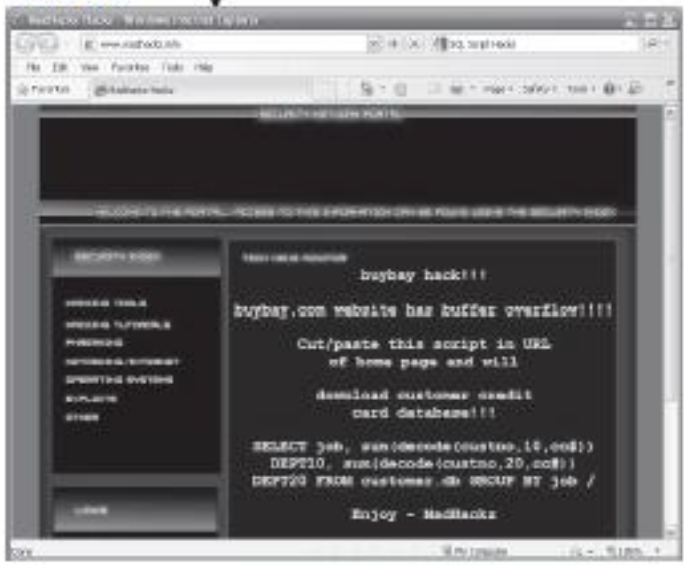
- Access
- Asset
- Attack
- Control, Safeguard, or Countermeasure
- Exploit
- Exposure
- Protection Profile or Security Posture
- Loss
- Hack
- Security Blueprint
- Security Model
- Risk
- Subjects and Objects
- Threat
- Threat Agent
- Vulnerability

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

Figure 1-4 Information Security Terms

Key Information Security Concepts (cont'd.)

- 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

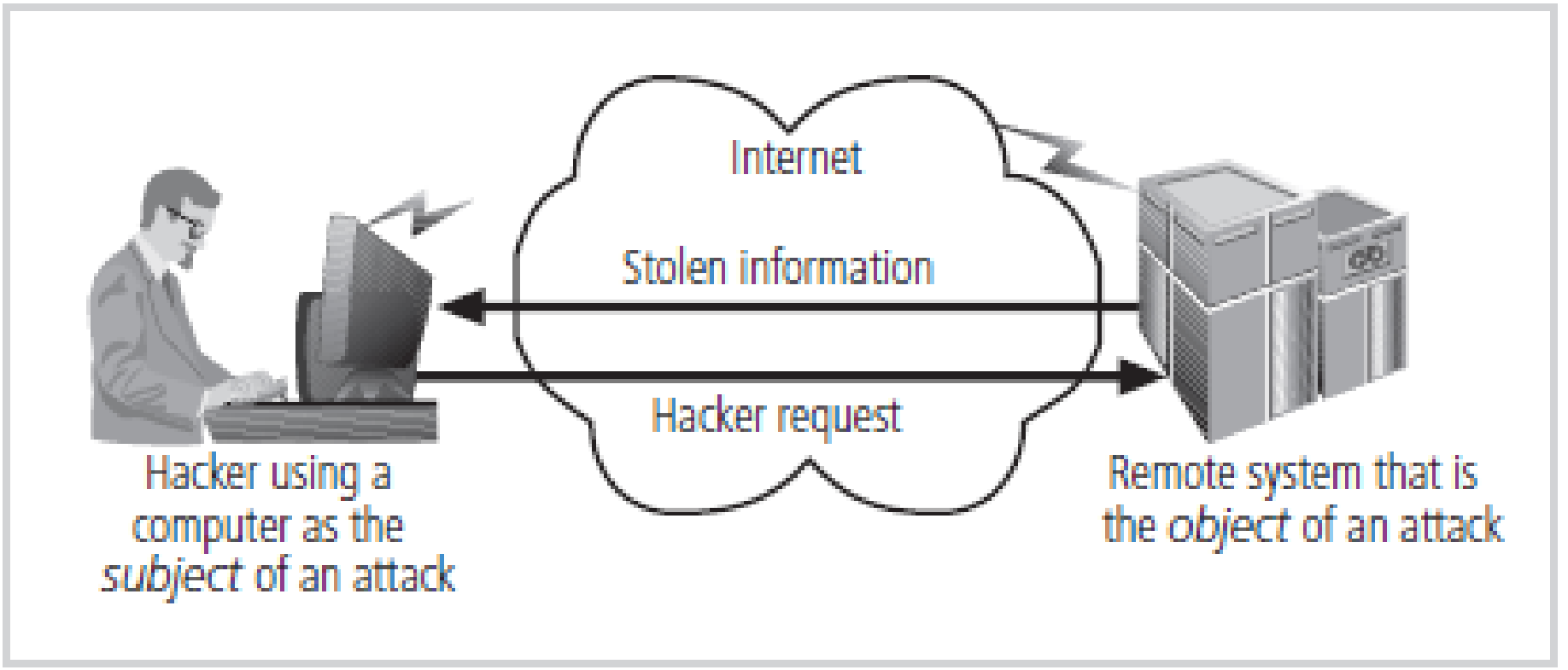


Figure 1-5 Computer as the Subject and Object of an Attack

Critical Characteristics of Information

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

CNSS Security Model

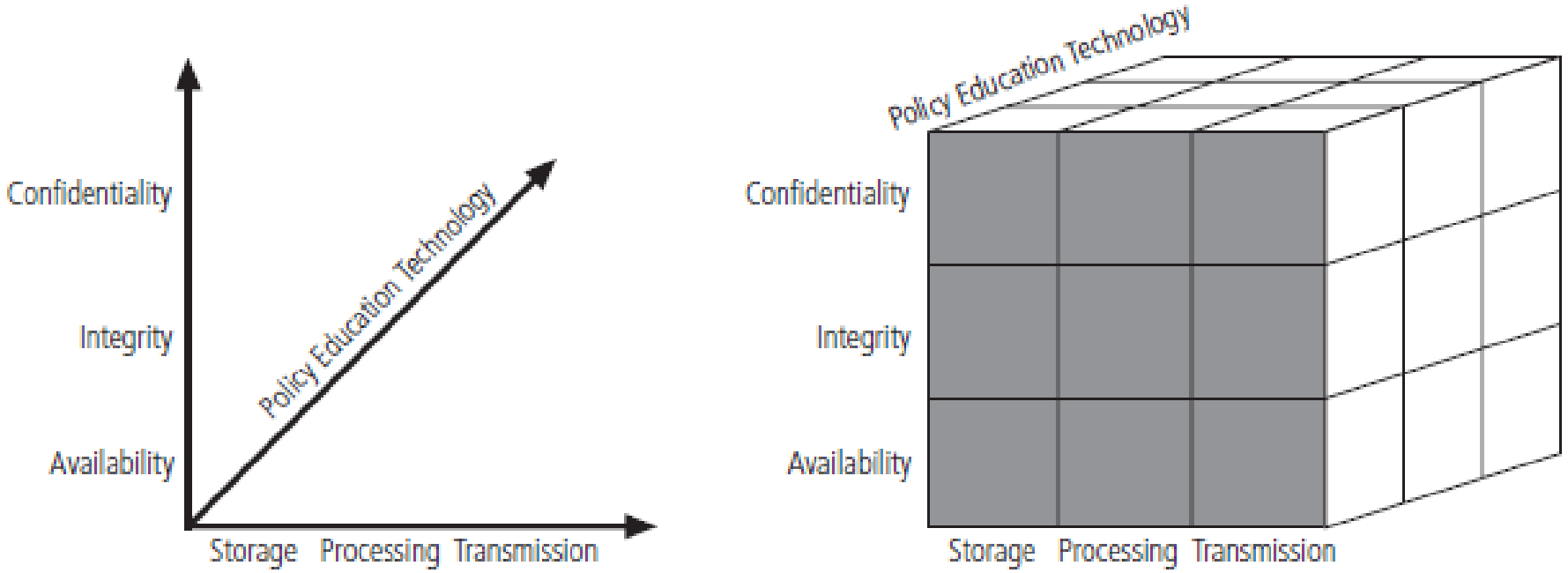


Figure 1-6 The McCumber Cube

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—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

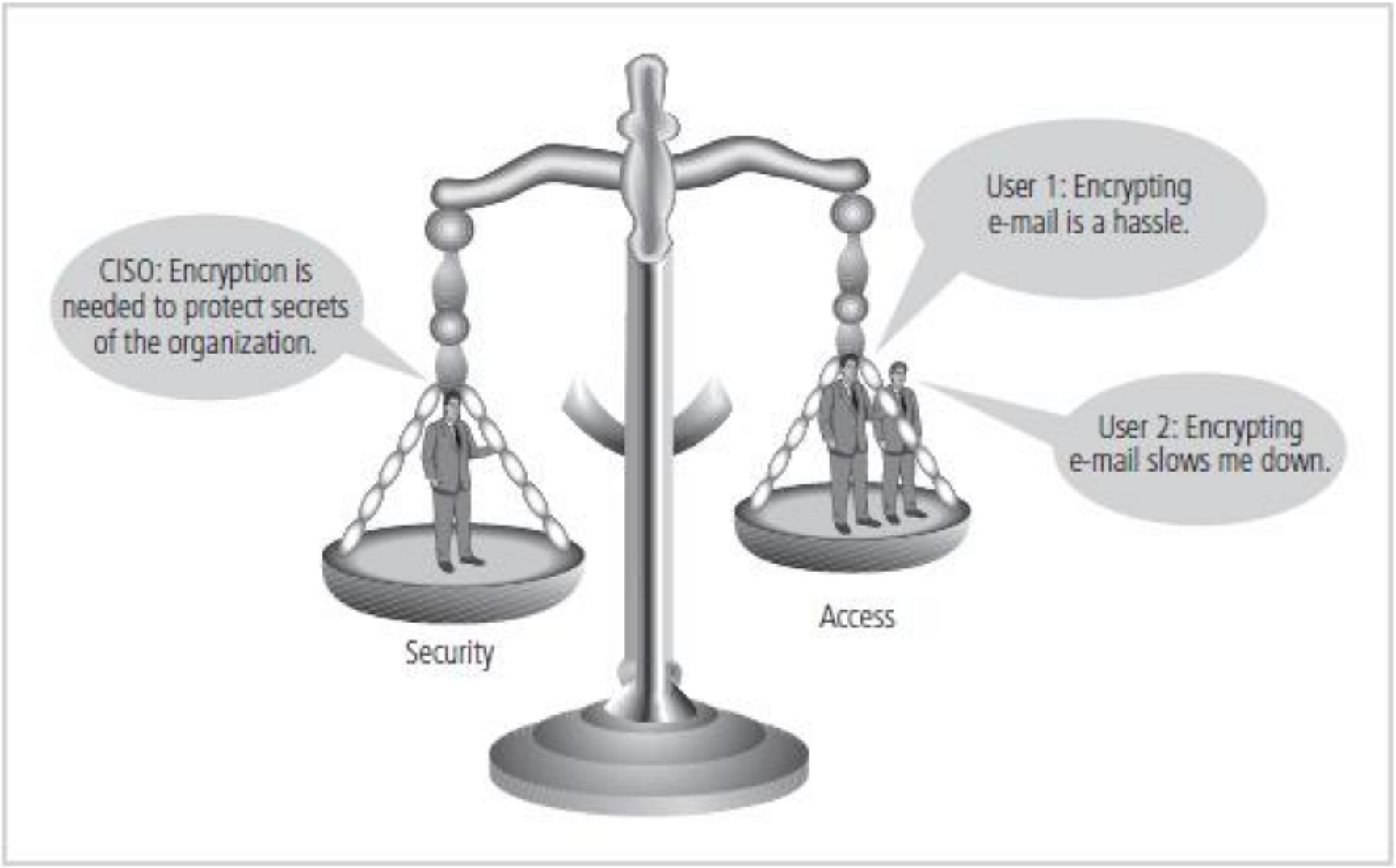


Figure 1-8 Balancing Information Security and Access

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

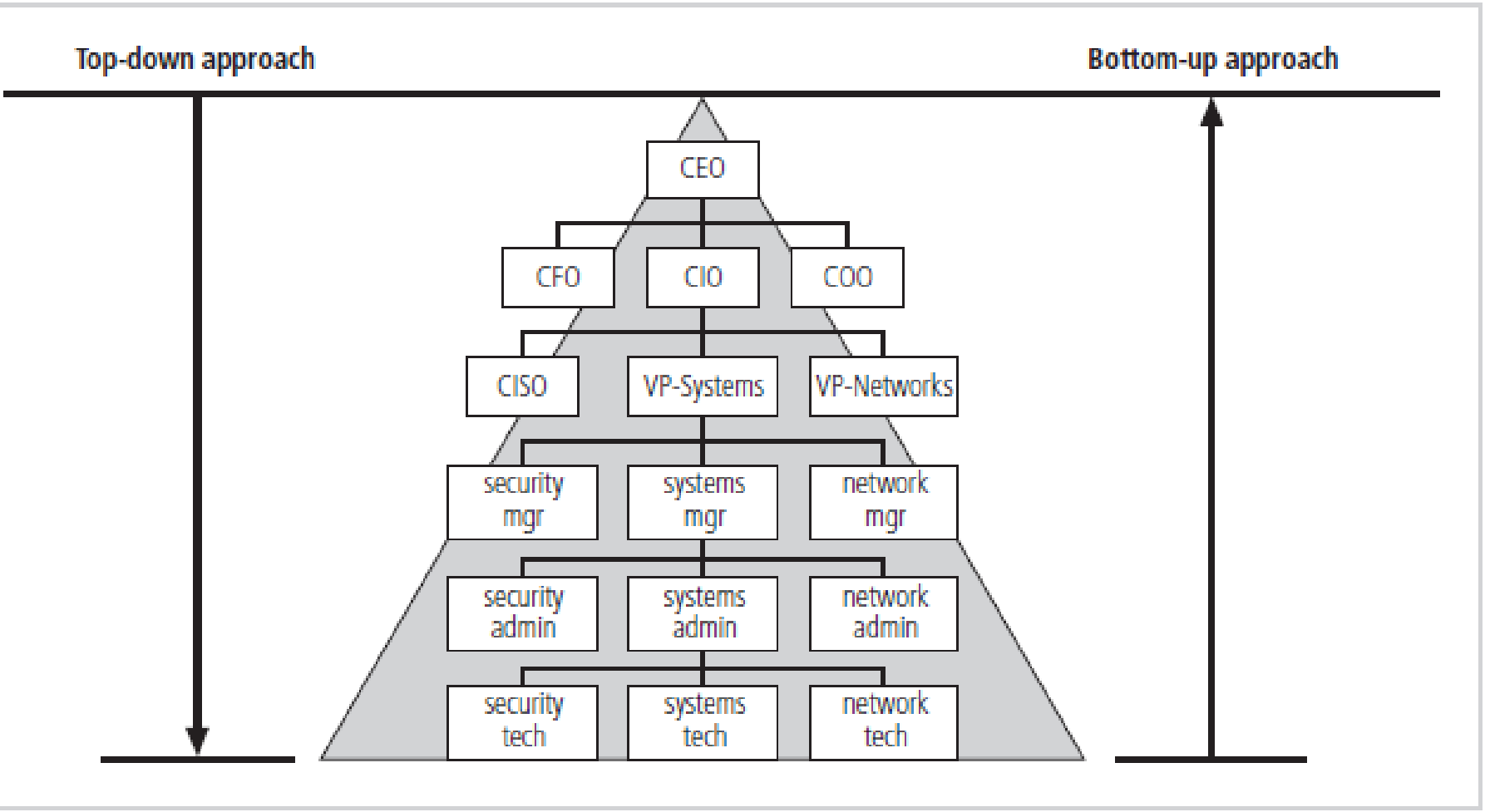


Figure 1-9 Approaches to Information Security Implementation

The Systems Development Life Cycle

- Systems Development Life Cycle (SDLC): methodology for design and implementation of information system within an organization
- 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

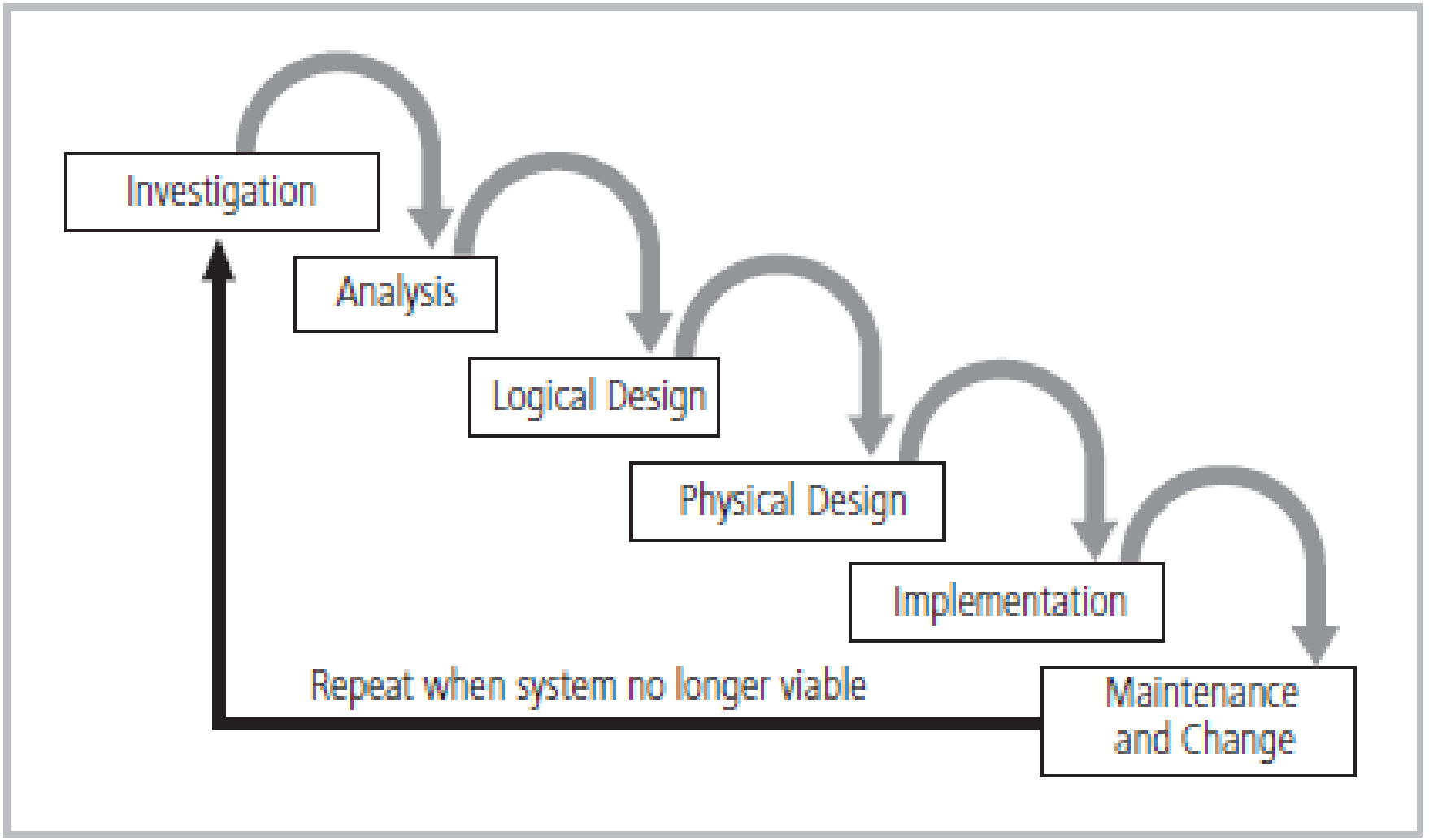


Figure 1-10 SDLC Waterfall Methodology

Investigation

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

Analysis

- Consists of assessments of:
  - The organization
  - Current systems
  - 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

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

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
- 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

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

Phases of the SecSDLC

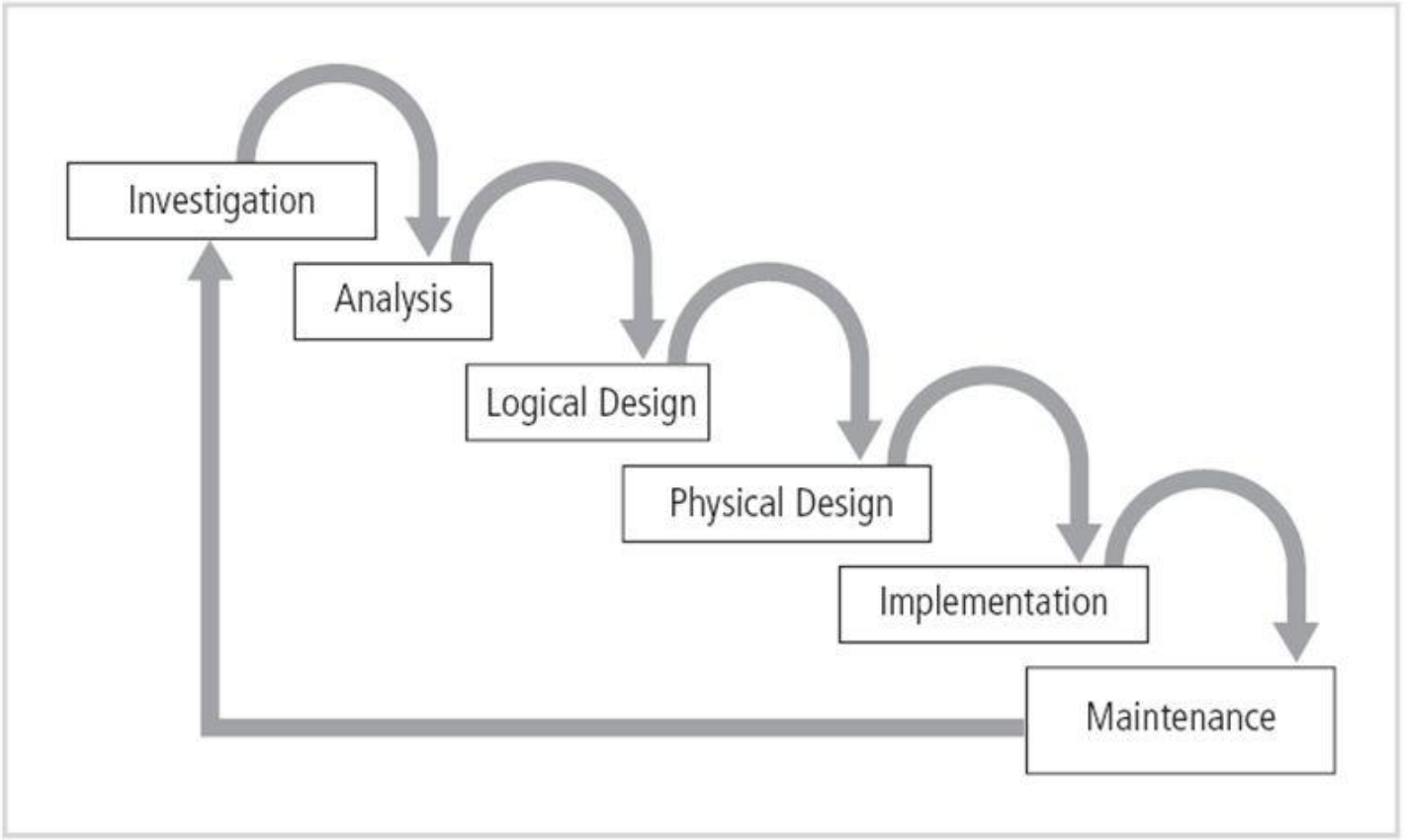


FIGURE 2-7 Phases of the SecSDLC

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

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

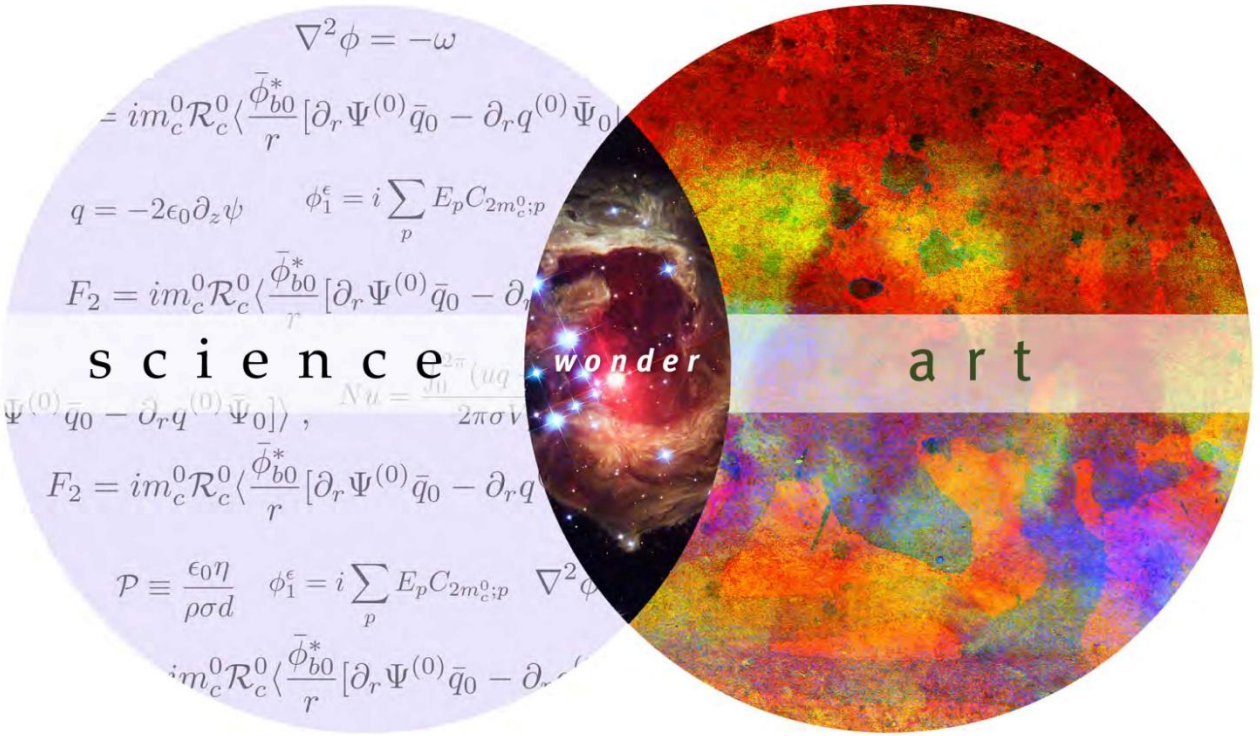
- Data owner: responsible for the security and use of a particular set of information
- Data custodian: responsible for storage, maintenance, and protection of information
- Data users: end users who work with information to perform their daily jobs supporting the mission of the organization

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

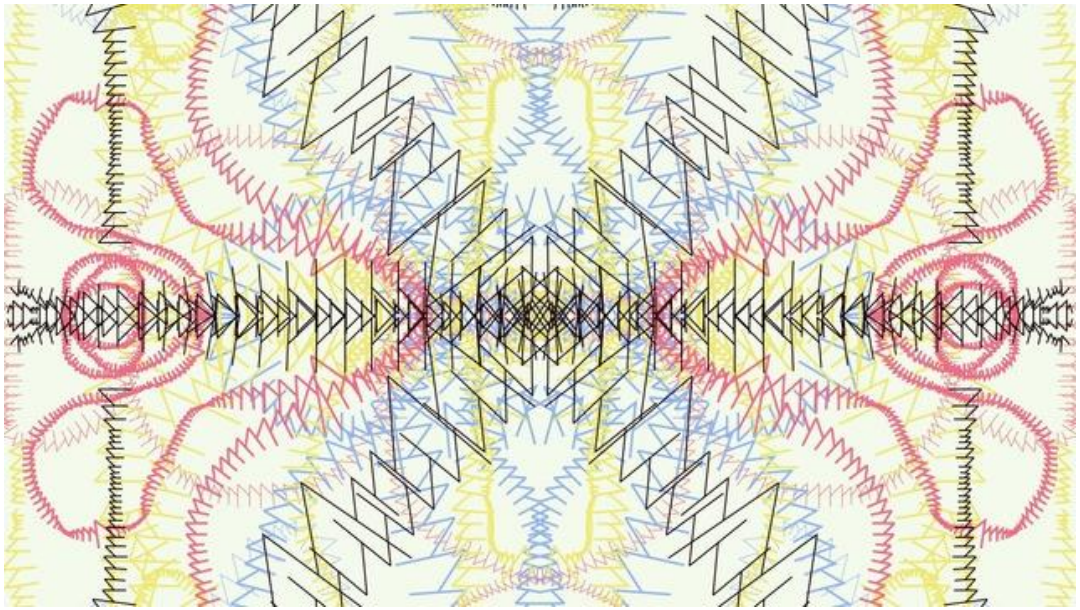
Information Security: Is it an Art or a Science?

- Implementation of information security often described as combination of art and science.



Security 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
- 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