Introduction to Information Security

Objectives

- Understand the definition of information security
- Comprehend the history of computer security and how it evolved into information security
- Understand the key terms and concepts of information security
- Outline the phases of the security systems development life cycle
- Understand the roles of professionals involved in information security 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)

The History of Information Security

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

The 1960s

- Advanced Research Procurement Agency (ARPA) began to examine feasibility of redundant networked communications

- Larry Roberts developed ARPANET from its inception

The 1970s and 80s

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

R-609

- 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

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

- In early Internet deployments, security was treated as a low priority

The Present

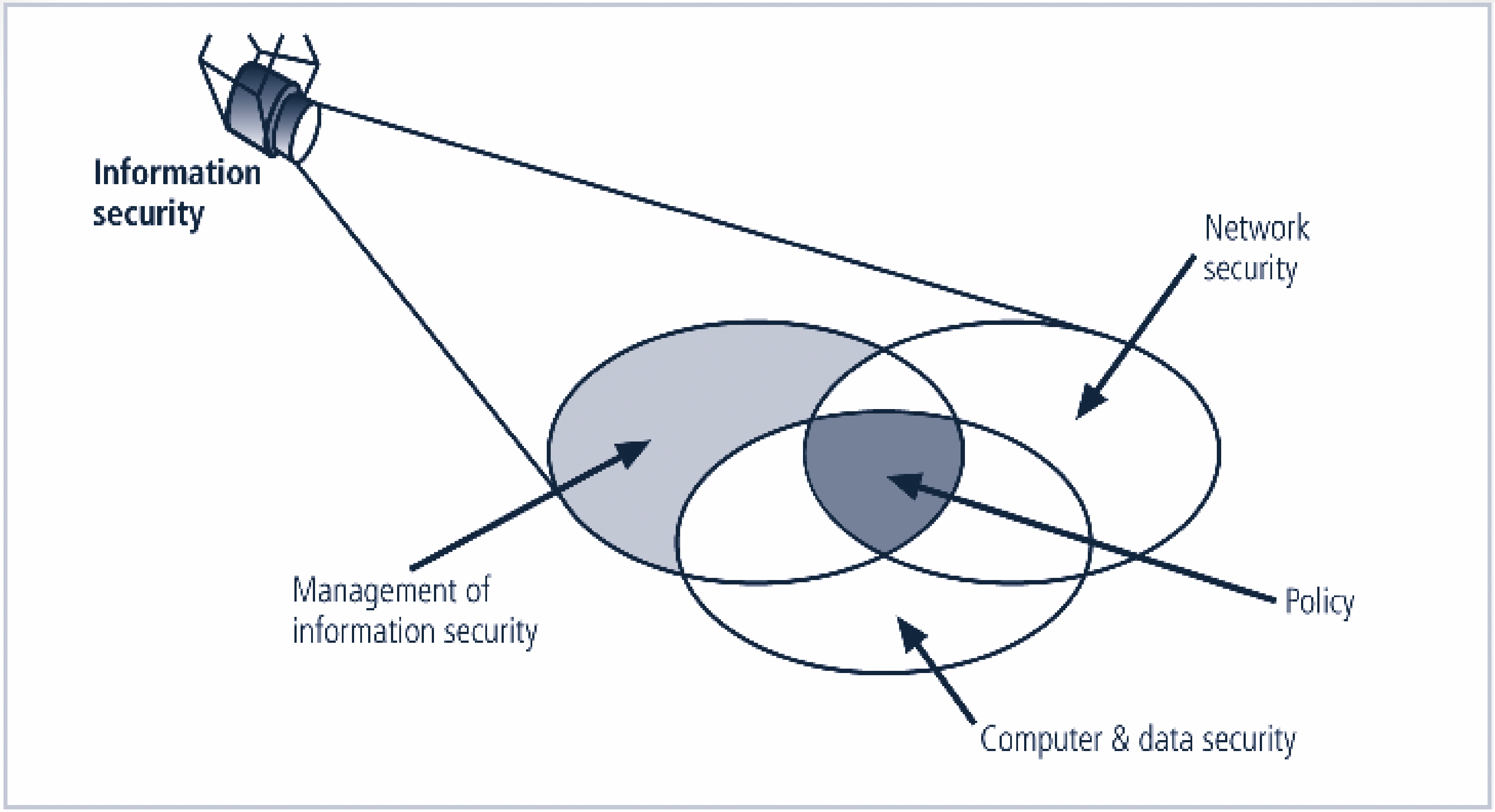
- The Internet brings millions of computer networks into communication with each other—many of them unsecured
- Ability to secure a computer’s data influenced by the security of every computer to which it is connected

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 Information Security?

- 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
- C.I.A. triangle now expanded into list of critical characteristics of information

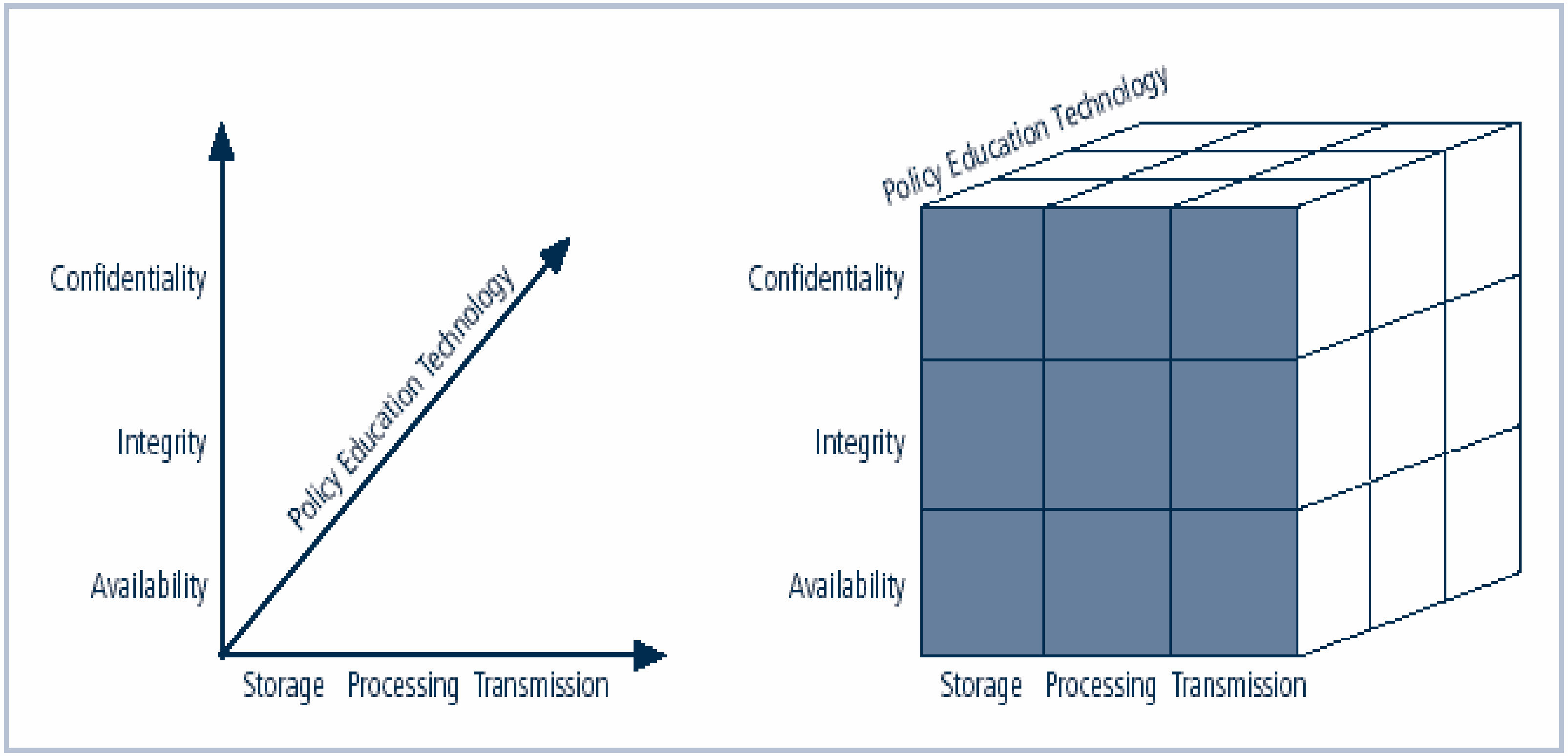


Components of Information Security

Critical Characteristics of Information

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

NSTISSC Security Model



NSTISSC Security Model

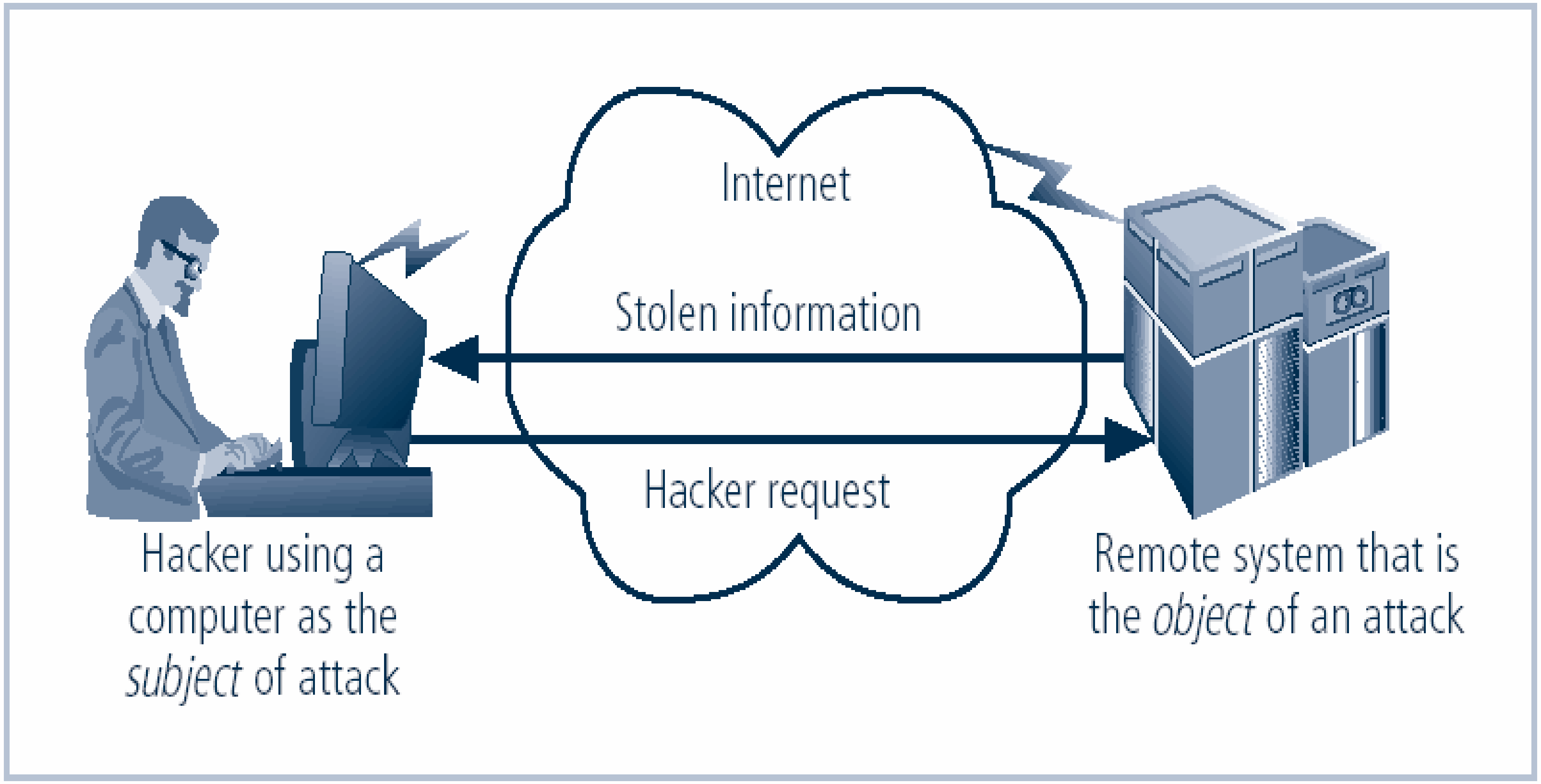
Components of an Information System

- Information System (IS) is entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization

Securing Components

- 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

F [illegible] ject


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

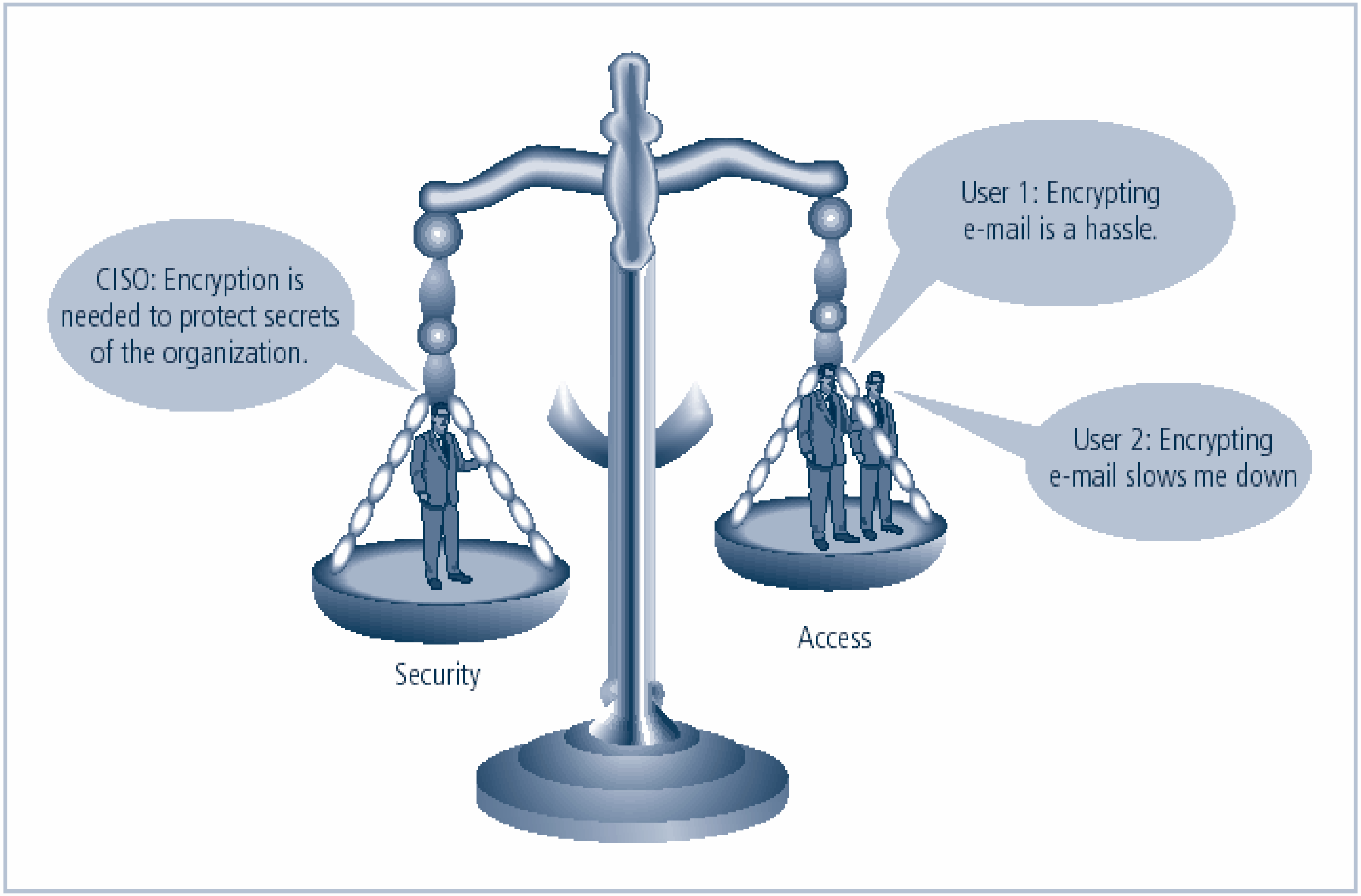
Computer as the Subject and Object of an Attack

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

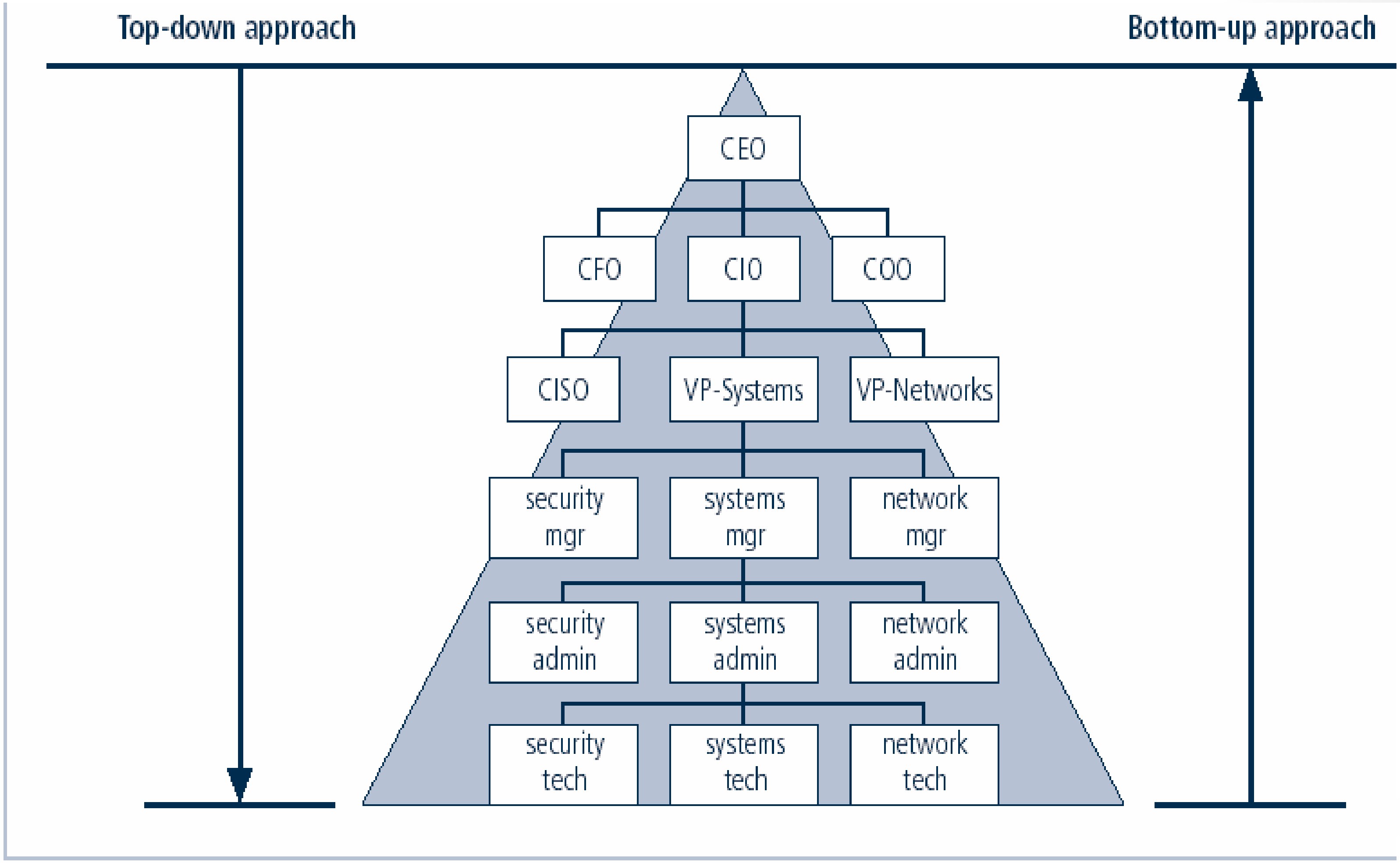
- To achieve balance, level of security must allow reasonable access, yet protect against threats


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

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