1

Introduction to Information Security

> Do not figure on opponents not attacking; worry about your own lack of preparation.
>
> **BOOK OF THE FIVE RINGS**

PRINCIPLES of INFORMATION SECURITY

Second Edition

Learning Objectives

Upon completion of this material, you should be able to:

- Understand the definition of information security
- Comprehend the history of computer security and how it evolved into information security
- Understand the key terms and critical concepts of information security as presented in the chapter
- 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)
- Necessary to review the origins of this field and its impact on our understanding of information security today

The History of Information Security

- Began immediately after the first mainframes were developed
- Created to aid code-breaking computations during World War II
- Physical controls to limit access to sensitive military locations to authorized personnel: badges, keys, and facial recognition
- Rudimentary in defending against physical theft, espionage, and sabotage

Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."

Courtesy of National Security Agency

FIGURE 1-1 The Enigma[2]

The History of Information Security

- One of 1st documented problems
  - Early 1960s
  - Not physical
  - Accidental file switch
    - Entire password file
    - printed on every output file

The 1960s

- Additional mainframes online
- Advanced Research Procurement Agency (ARPA) began to examine feasibility of redundant networked communications
- Larry Roberts developed ARPANET from its inception
- ARPANET is the first Internet

ARPANET Program Plan

June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. **Objectives – Develop Networking and Resource Sharing**
2. **Technical Need – Linking Computers**
3. **Military Need – Resource Sharing - Not Nuclear War**
4. **Prior Work – MIT-SDC experiment**
5. **Effect on ARPA – Link 17 Computer Research Centers, Network Research**
6. **Plan - Develop IMP's and start 12/69**
7. **Cost – $3.4 M for 68-71**

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

Courtesy of Dr. Lawrence Roberts

FIGURE 1-2 ARPANET Program Plan[4]

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

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
    - First identified role of management and policy

The History of Information Security

- Multics
  - Operating System
  - Security primary goal
  - Didn't go very far
  - Several developers created Unix
- Late 1970s: microprocessor expanded computing capabilities and security threats
  - From mainframe to PC
  - Decentralized computing
  - Need for sharing resources increased
  - Major changed computing

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
  - Many of the problems that plague e-mail on the Internet are the result to this early lack of security

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

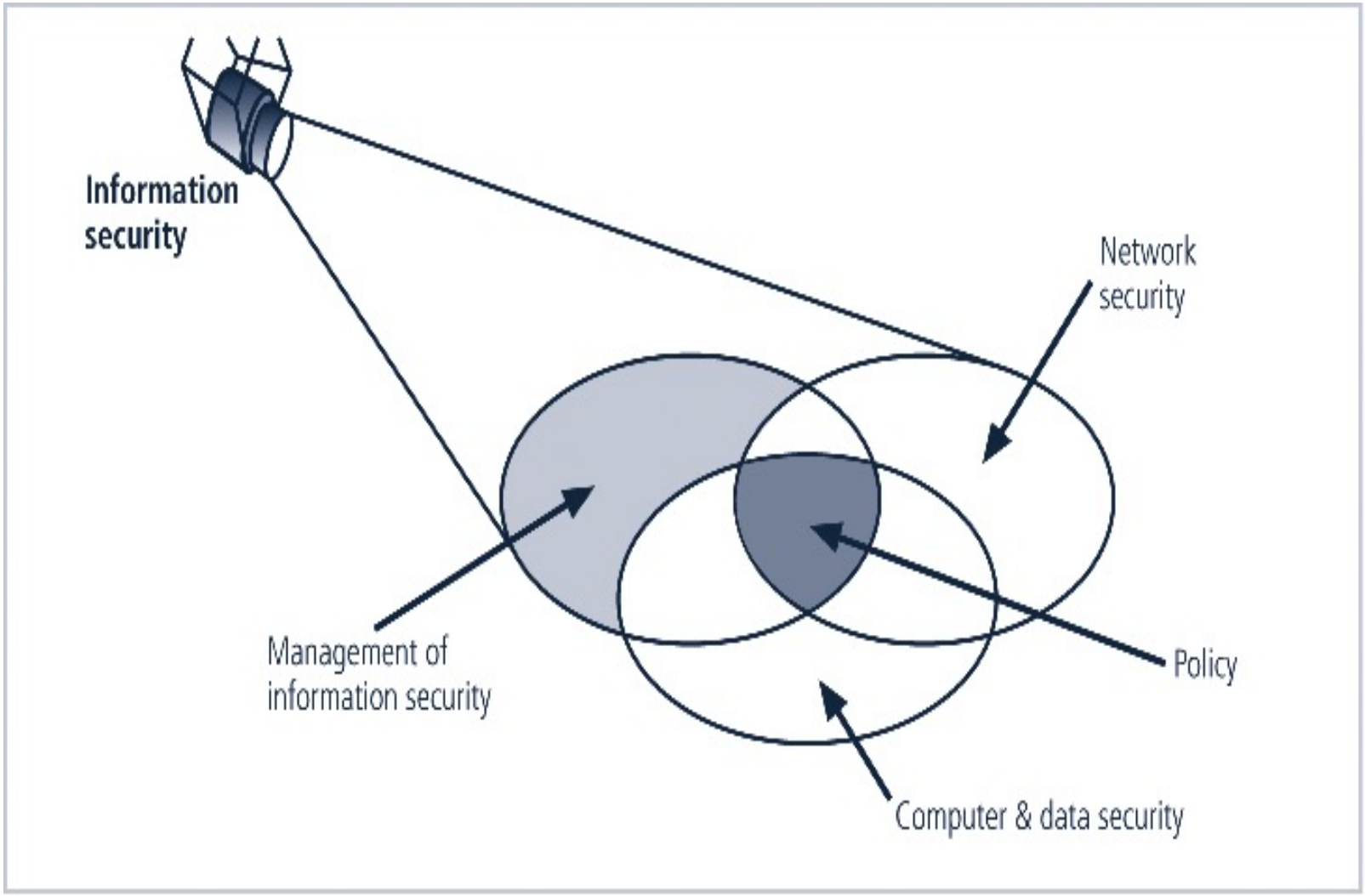

FIGURE 1-3 Components of Information Security

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
  - Timeliness
    - No value if it is too late
  - Availability
    - No interference or obstruction
    - Required format
  - Accuracy
    - Free from mistakes
  - Authenticity
    - Quality or state of being genuine, i.e., sender of an email
  - Confidentiality
    - Disclosure or exposure to unauthorized individuals or system is prevented

Critical Characteristics of Information

- Integrity
  - Whole, completed, uncorrupted
  - Cornerstone
  - Size of the file, hash values, error-correcting codes, retransmission
- Utility
  - Having value for some purpose
- Possession
  - Ownership
  - Breach of confidentiality results in the breach of possession, not the reverse

NSTISSC Security Model

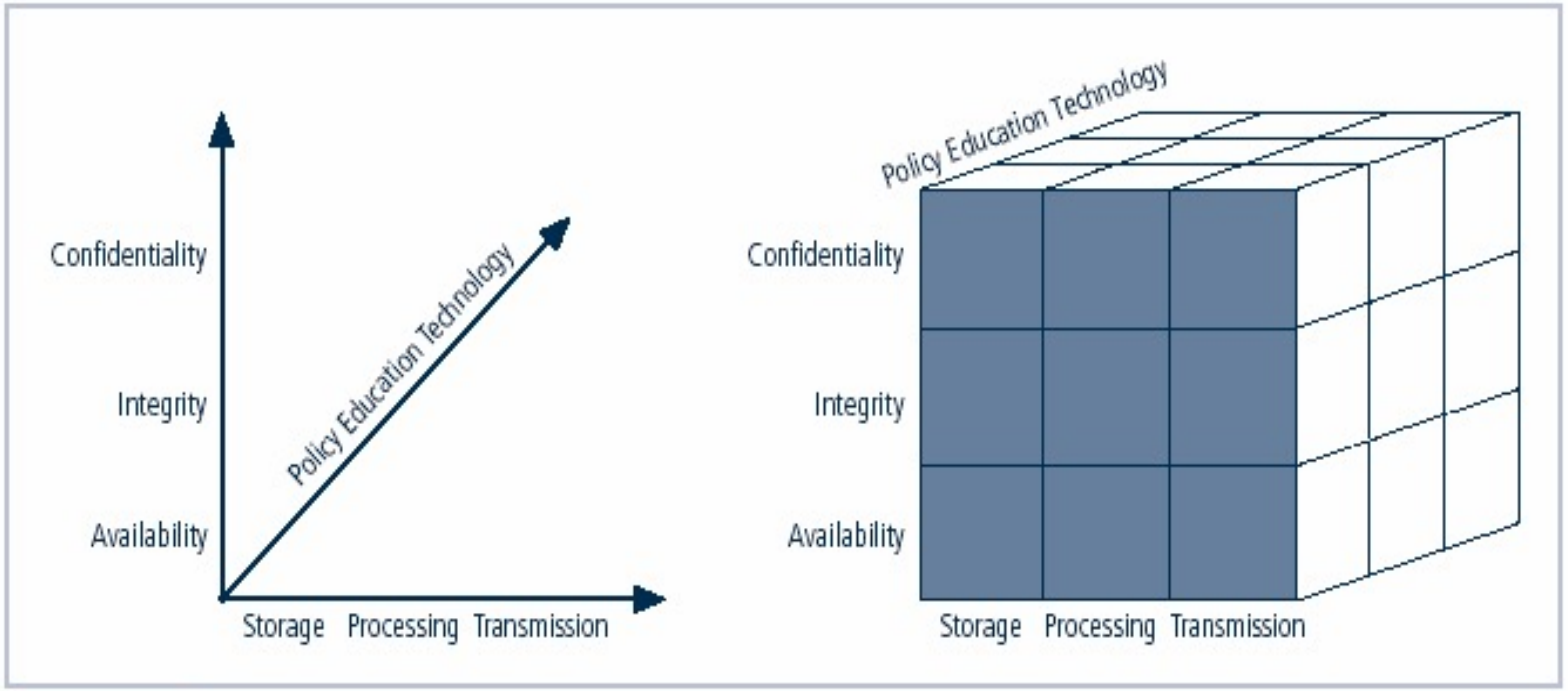

FIGURE 1-4 NSTISSC Security Model

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
- Software
  - Perhaps most difficult to secure
  - Easy target
  - Exploitation substantial portion of attacks on information
- Hardware
  - Physical security policies
  - Securing physical location important
  - Laptops
  - Flash memory

Components of an Information System

- Data
  - Often most valuable asset
  - Main target of intentional attacks
- People
  - Weakest link
  - Social engineering
  - Must be well trained and informed
- Procedures
  - Threat to integrity of data
- Networks
  - Locks and keys won't work

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
- 2 types of attack
  - Direct
    - Hacker uses their computer to break into a system
  - Indirect
    - System is compromised and used to attack other systems

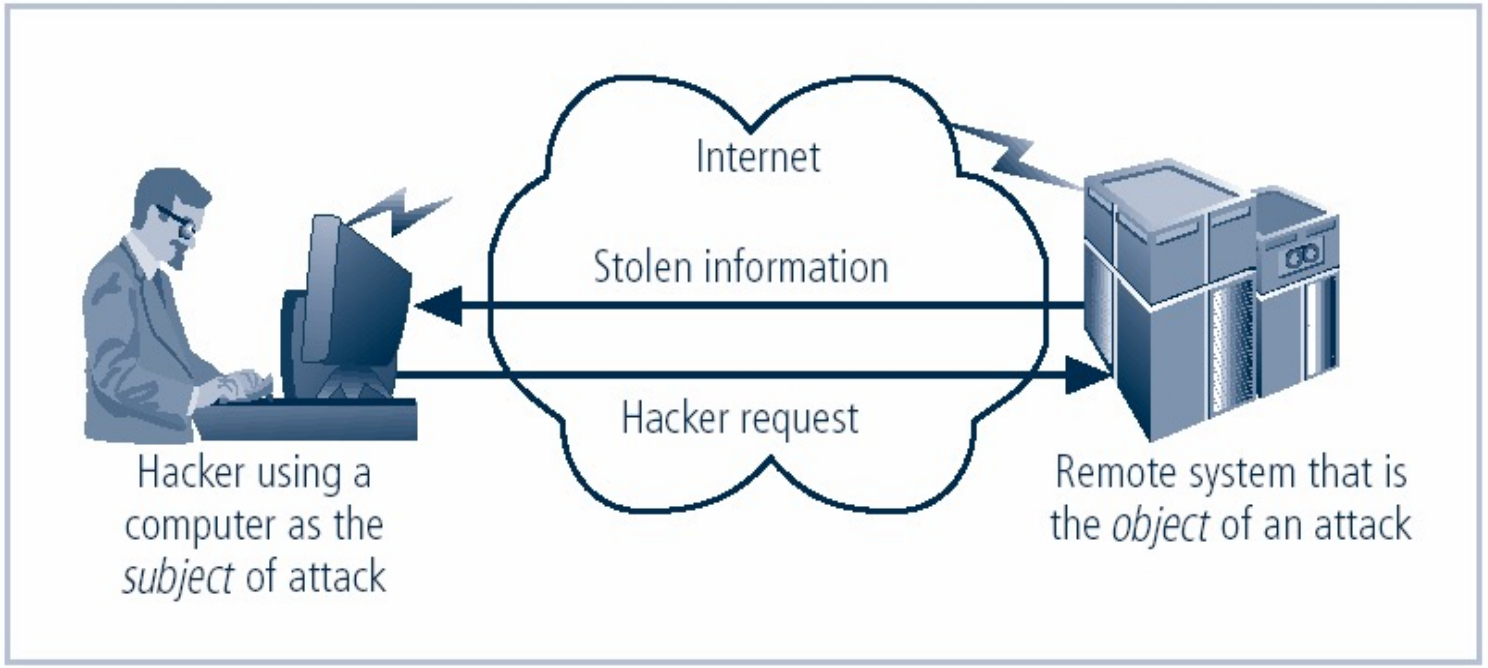

FIGURE 1-6 Computer as the Subject and Object of an Attack

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

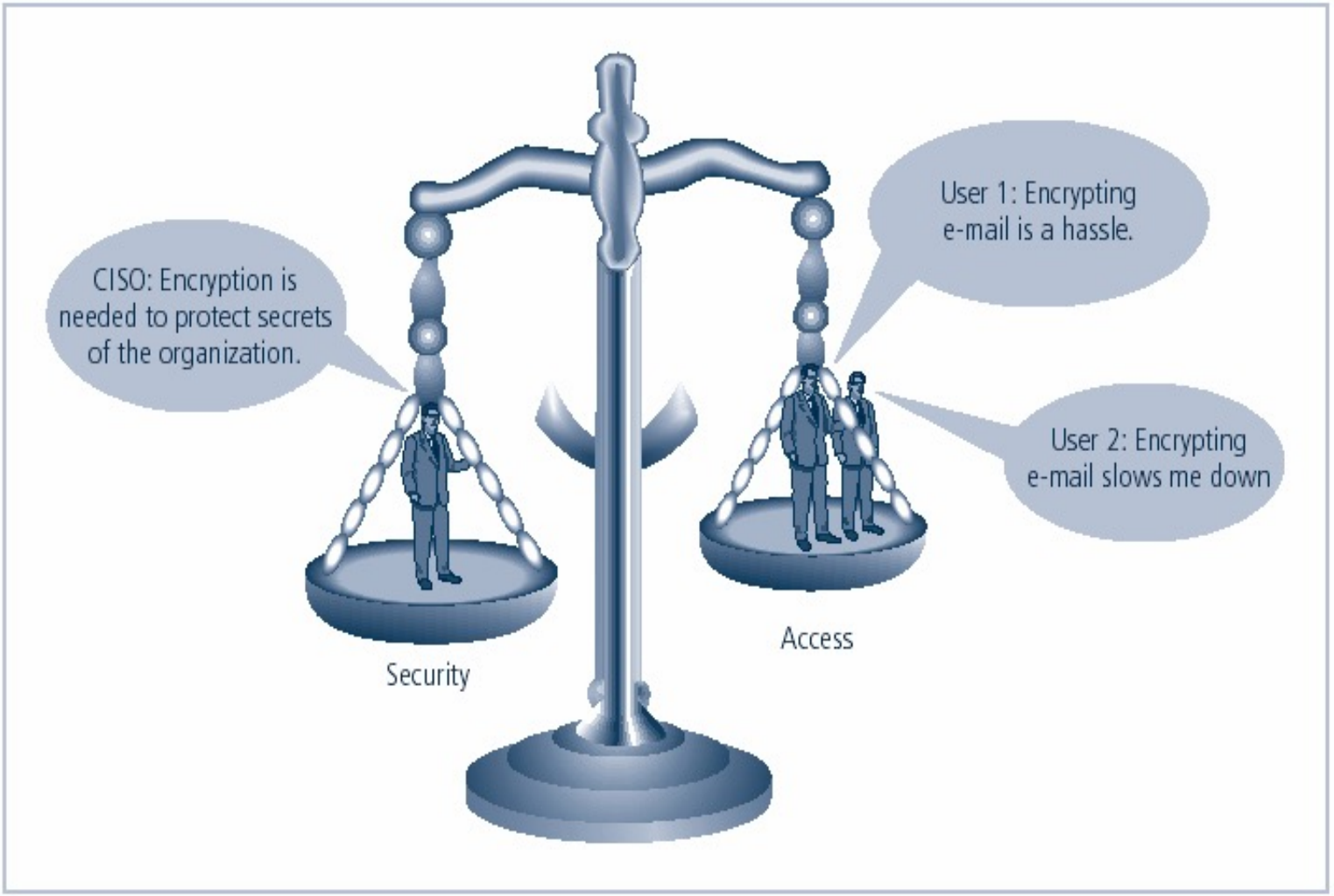

FIGURE 1-7 Balancing Information Security and Access

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

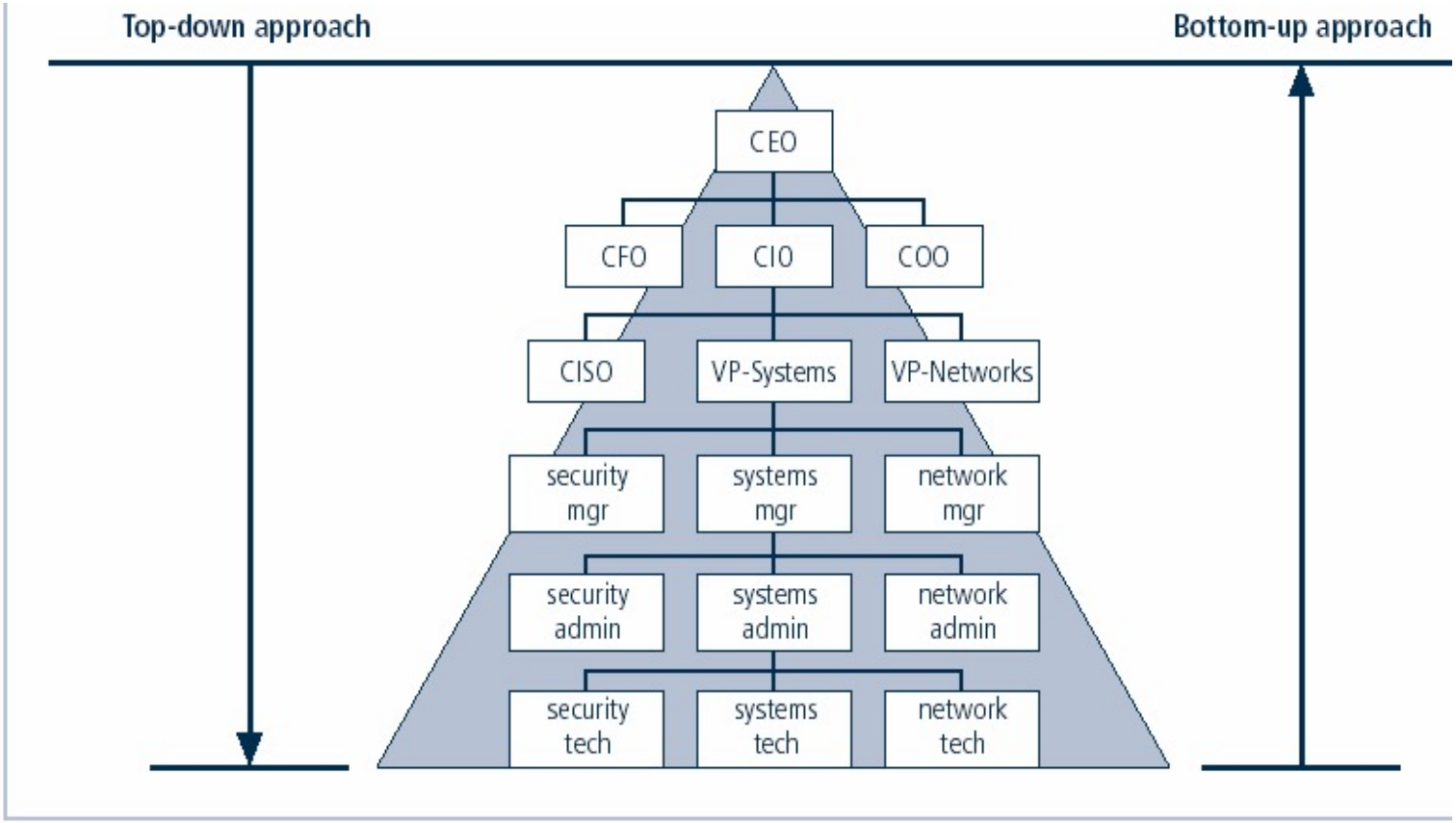

FIGURE 1-8 Approaches to Information Security Implementation

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

The Systems Development Life Cycle

- Systems development life cycle (SDLC) is methodology and design for implementation of information security within an organization
- Methodology is formal approach to problem-solving based on structured sequence of procedures
- Using a methodology
  - ensures a rigorous process
  - avoids missing steps
- Goal is creating a comprehensive security posture/program
- Traditional SDLC consists of six general phases

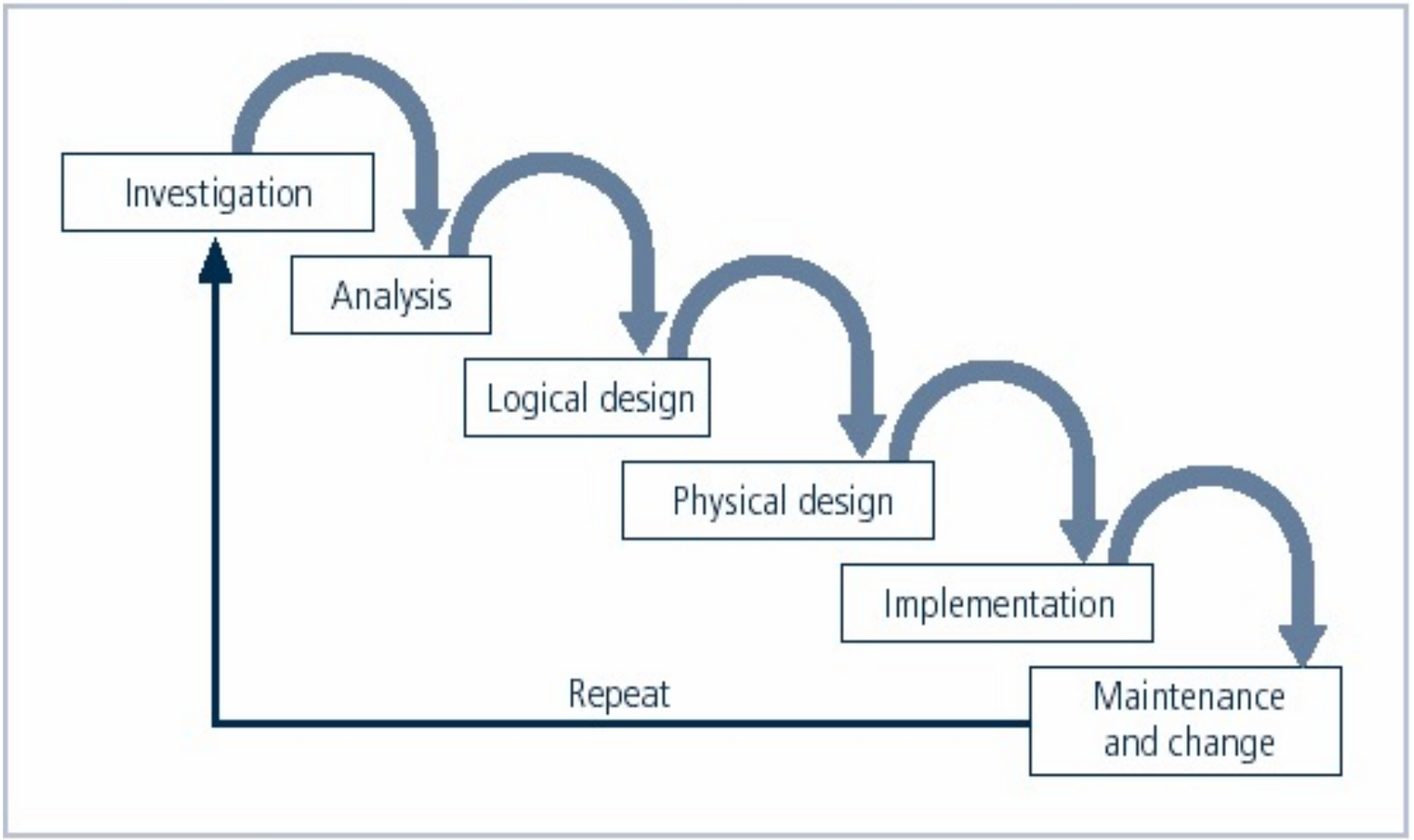

FIGURE 1-9 SDLC Waterfall Methodology

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

The Security Systems Development Life Cycle

- Investigation
  - Identifies process, outcomes, goals, and constraints of the project
  - Begins with enterprise information security policy
- Analysis
  - Existing security policies, legal issues,
  - Perform risk analysis

The Security Systems Development Life Cycle

- Logical Design
  - Creates and develops blueprints for information security
  - Incident response actions: Continuity planning, Incident response, Disaster recovery
  - Feasibility analysis to determine whether project should continue or be outsourced
- Physical Design
  - Needed security technology is evaluated, alternatives generated, and final design selected

The Security Systems Development Life Cycle

- 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
  - Most important
  - Constant changing threats
  - Constant monitoring, testing updating and implementing change

Security Professionals and the Organization

- Wide range of professionals required to support a diverse information security program
- Senior management is key component; also, additional administrative support and technical expertise 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 technical and non-technical areas:
  - Champion: Senior executive who promotes the project
  - Team leader: project manager, departmental level manager
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems administrators
  - End users

Data Ownership

- 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 interest/values in an organization
  - Information Security Management and Professionals
  - Information Technology Management and Professionals
  - Organizational Management and Professionals

Key Terms

- Access
- Asset
- Attack
- Control, Safeguard or Countermeasure
- Exploit
- Exposure
- Hacking
- Object
- Risk
- Security Blueprint
- Security Model
- Security Posture or Security Profile
- Subject
- Threats
- Threat Agent
- Vulnerability

Critical infrastructure

- From Wikipedia.
- Critical infrastructure is a term used by governments to describe systems or material assets that are essential for the functioning of a society and economy. Most commonly associated with the term are facilities for:
- electricity generation and distribution;
- telecommunication;
- water supply;
- agriculture, food production and distribution;
- heating (natural gas, fuel oil);
- public health;
- transportation systems (fuel supply, railway network, airports);
- financial services;
- security services (police, military).
- Critical-infrastructure protection is the study, design and implementation of precautionary measures aimed to reduce the risk that critical infrastructure fails as the result of war, disaster, civil unrest, vandalism, or sabotage.

Summary

- Information security is a “well-informed sense of assurance that the information risks and controls are in balance.”
- Computer security began immediately after first mainframes were developed
- Successful organizations have multiple layers of security in place: physical, personal, operations, communications, network, and information.

Summary

- Security should be considered a balance between protection and availability
- Information security must be managed similar to any major system implemented in an organization using a methodology like SecSDLC
- Implementation of information security often described as a combination of art and science