

Chapter 1: Introduction to computer security and privacy

Faris a.

Learning Objectives

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

- Understand the definition of information security

- Understand the key terms and critical concepts of information security

- Comprehend the history of computer security and how it evolved into information security

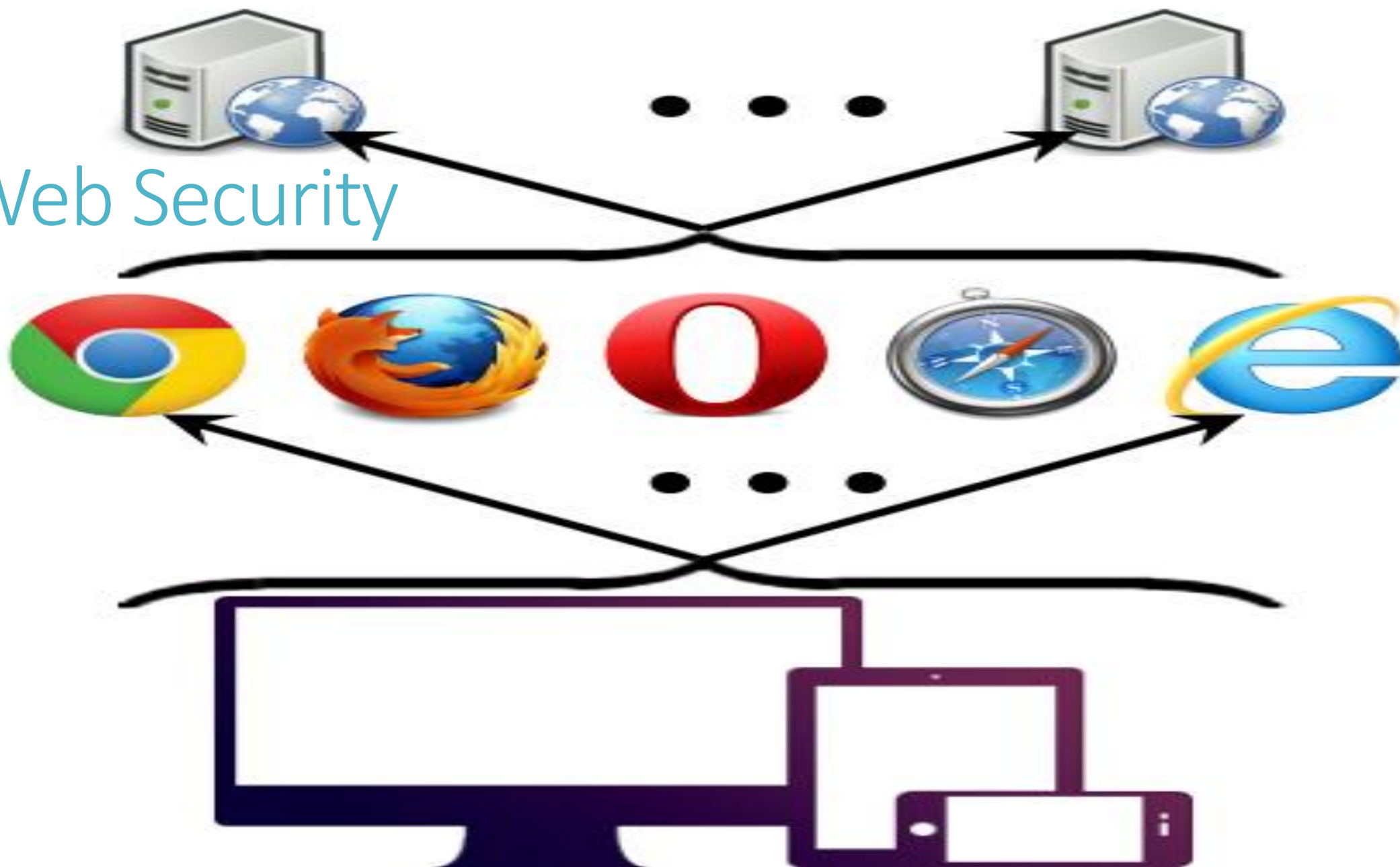
What is an Information System?

Information System (IS): an entire set of

- Software
- Hardware
- Data
- People
- Procedures, and
- Networks

necessary to use information within an organization

Web Security





Mobile Device Security


Organization

Sprint



T-Mobile



facebook

☐ Keep me logged in

[Forgot your password?](#)

Email

Login

Facebook helps you connect and share with the people in your life.

Sign Up

It's free and anyone can join

First Name:

Last Name:

Your Email:

New Password:

I am: Select Sex:

Birthday: Month: Day: Year:

Why do I need to provide this?

[Create a Page for a celebrity, band or business.](#)

Social Networking Security

[English \(US\)](#) [Español](#) [Português \(Brasil\)](#) [Français \(France\)](#) [Deutsch](#) [Italiano](#) [العربية](#) [हिन्दी](#) [한국어](#) [日本語](#) [繁體中文](#) [简体中文](#) [更多语言](#) >>

Facebook © 2010 English (US)

[About](#) [Advertising](#) [Developers](#) [Careers](#) [Terms](#) • [Find Friends](#) [Privacy](#) [Mobile](#) [Help Center](#) [Blog](#) [Badges](#)

do you have a facebook?

“Giving people the power to share and make the world more open and connected.”



Critical Characteristics of Information

The value of information comes from its characteristics:

- Confidentiality**
- Integrity**: (Bitwise) identical to the original
- Availability**: of info, services, etc.
- Authenticity**: “it is what it claims to be”
- Accuracy**: free from mistakes and errors
- Utility**:
- Possession**: different from confidentiality

Others:

- User authentication: users are who they claim to be
- Auditability: there’s a record of who accessed what
- Non-repudiation: one cannot claim “I didn’t sign this”

What is Security?

- Definitions:

Book: “The quality or **state of being secure**—to be free from danger”

James Anderson, Inovant: “Well-informed sense that information **risks** and **controls** are in **balance**”

Rita Summers, IBM Systems Journal, 1984: “Includes **concepts**, **techniques** and **measures** that are used to **protect** computing systems and the information they maintain against deliberate or accidental **threats**”

- Successful companies should have multiple security “tiers”:

- **Physical** security
- **Personal** security
- **Operations** security
- **Communications** security
- **Network** security
- **Information** security

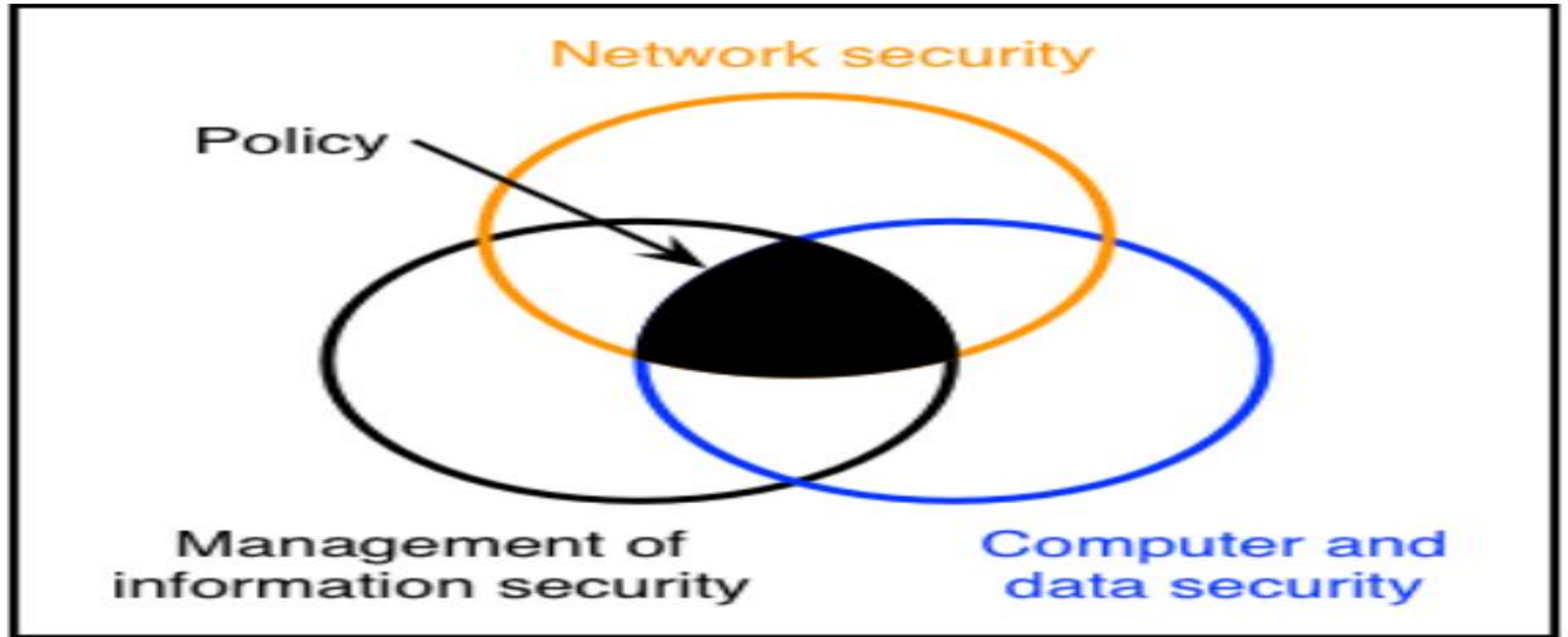
What is Information Security?

- Protection of information and its critical elements, including systems that use, store, and transmit that info

Necessary tools:

- **Policy**
- Awareness
- Training
- Education
- Technology

Aspects of information security



Securing Components in an Information System

Computers (**software** and **hardware**): key components in an IS

Computers can be subjects and/or objects of an attack:

Subject of an attack: attackers use computers actively to **launch** attacks against targets

Object of an attack: computers are what are under attack!

Key Information Security Concepts

- Access: A subject or object's ability to use, manipulate, modify, or affect another subject or object. Authorized users have legal access to a system, whereas hackers have illegal access to a system. Access controls regulate this ability.
- Asset: The organizational resource that is being protected.
- An asset can be logical, such as a Web site, information, or data; or an asset can be physical, such as a person, computer system, or other tangible object. Assets, and particularly information assets, are the focus of security efforts; they are what those efforts are attempting to protect.
- Attack: An **intentional** or **unintentional** act that can cause damage to or otherwise compromise information and/or the systems that support it. Attacks can be **active** or **passive**, **intentional** or **unintentional**, and **direct** or **indirect**.

cont

Control, safeguard, or countermeasure: Security mechanisms, policies, or procedures that can successfully **counter attacks, reduce risk, resolve vulnerabilities**, and otherwise **improve** the security within an organization.

Exploit: A technique used to **compromise** a system. This term can be a verb or a noun. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain. Or, an exploit can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or is created by the attacker. Exploits make use of existing software tools or custom-made software components.

Exposure: A **condition** or **state** of being exposed. In information security, exposure exists when a vulnerability known to an attacker is present.

Loss: A single **instance of an information asset suffering damage** or unintended or unauthorized modification or disclosure. When an organization's information is stolen, it has suffered a loss.

Protection profile or security posture: The entire set of controls and safeguards, including policy, education, training and awareness, and technology, that the organization implements (or fails to implement) to protect the asset. The terms are sometimes used interchangeably with the term security program,

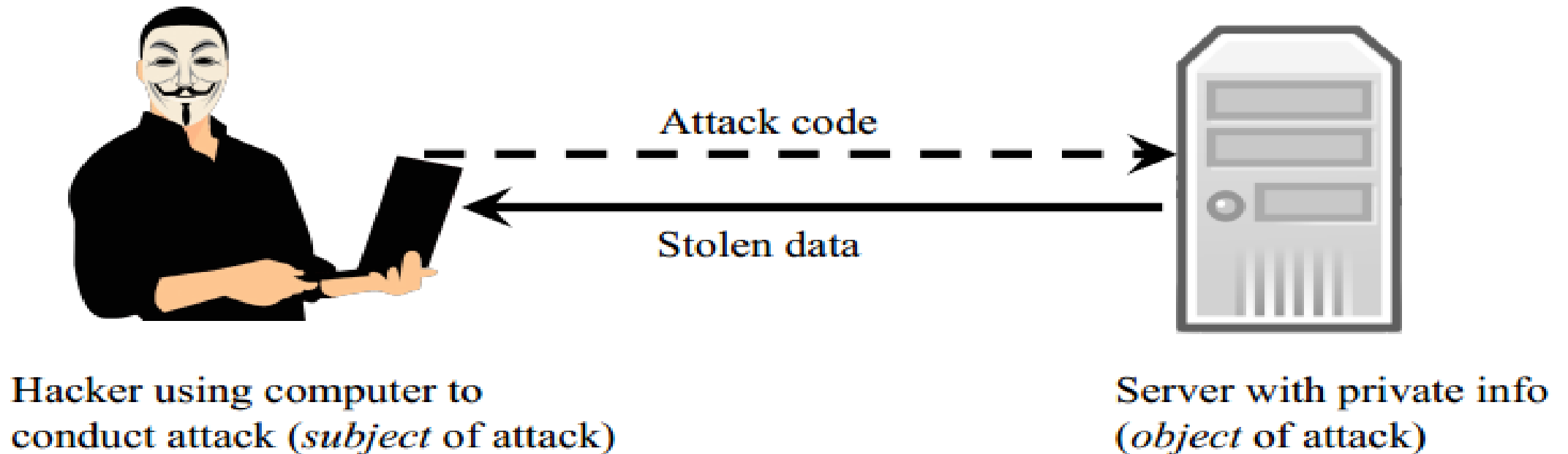
Risk: The **probability** that something unwanted will happen. Organizations must minimize risk to match their **risk appetite**—the quantity and nature of risk the organization is willing to accept

Vulnerability: A **weaknesses** or fault in a system or protection mechanism that opens it to attack or damage.

Threat: A category of objects, persons, or other entities that presents a danger to an asset. Threats are always **present** and can be **purposeful** or **undirected**.

Threat agent: The specific instance or a **component** of a threat.

Computers: Subjects/Objects of Attack

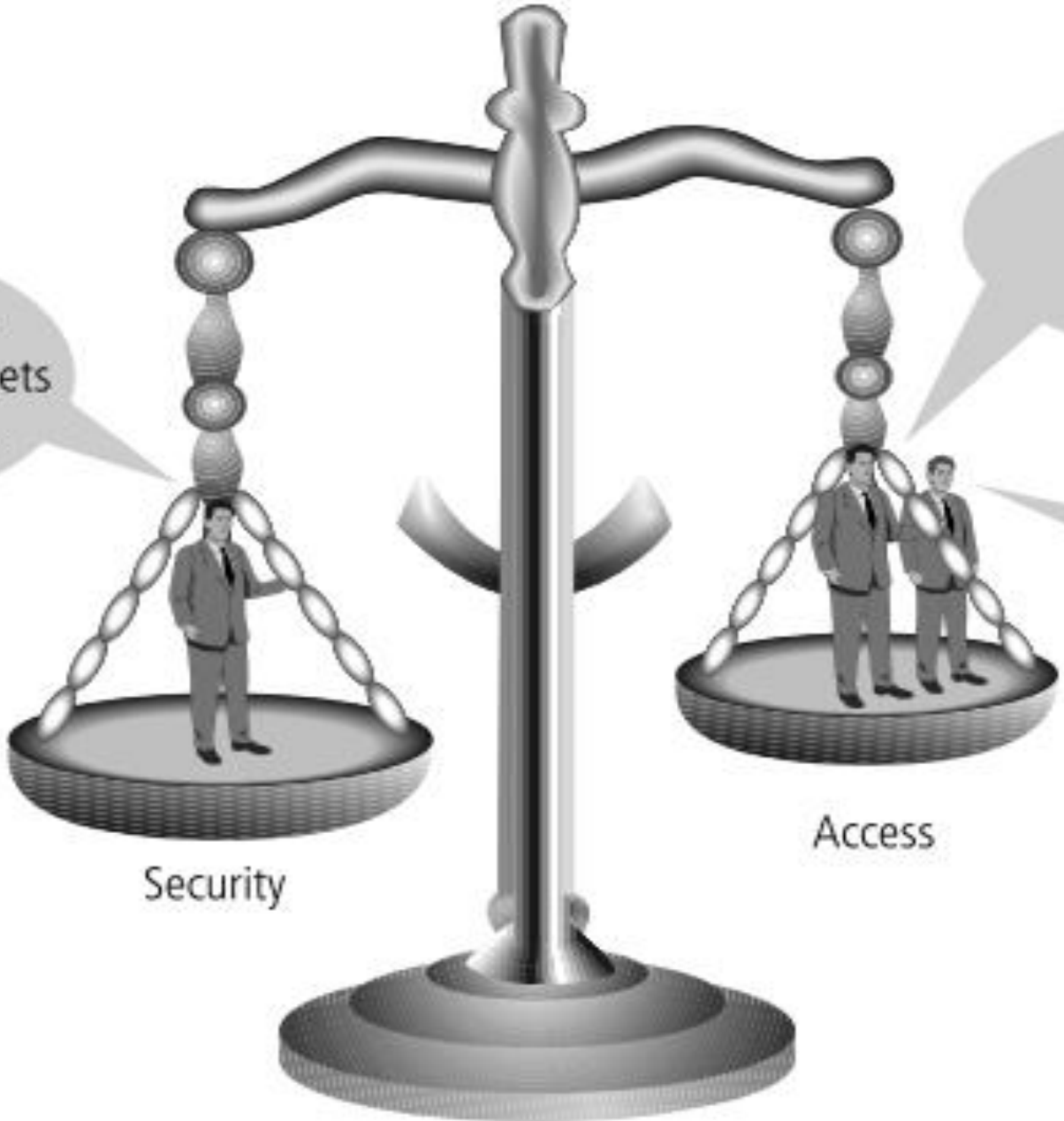


Balancing Information Security and Access

Impossible to obtain perfect security: it's 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



A balance scale is shown with two pans. The left pan, labeled 'Security', is lower and contains one person. The right pan, labeled 'Access', is higher and contains two people. The scale is tilted towards the 'Security' side. A curved arrow indicates the scale's movement. Three speech bubbles are present: one from the person on the 'Security' pan, and two from the people on the 'Access' pan.

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

Security vs. Access Security

Security

- CIO: Two-factor authentication is necessary to protect private data
- Auditor: We need to comply with laws/regulations

Access

- Student 1: I forgot my authentication device
- Student 2: It's a hassle

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

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 1980s

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

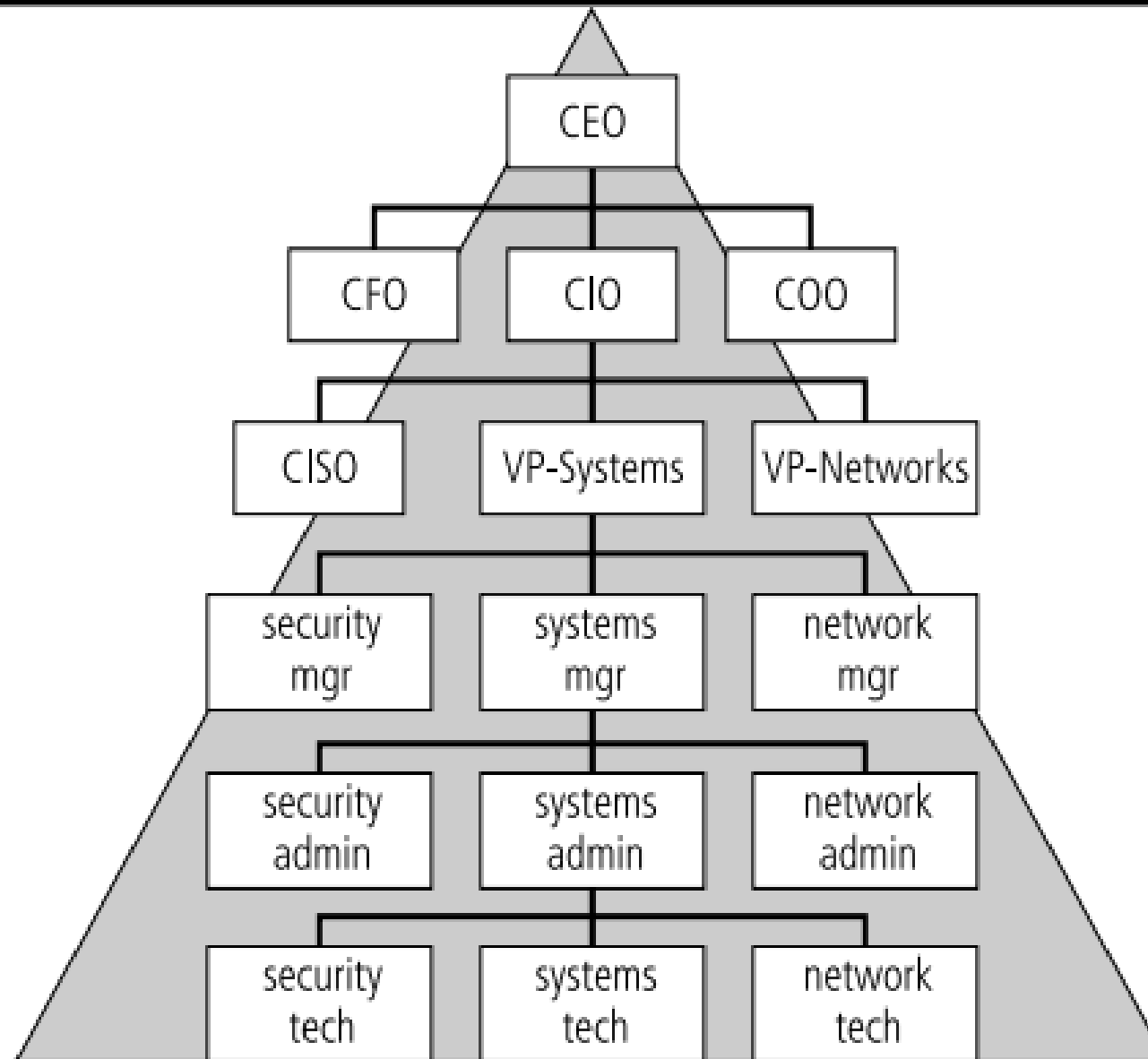
The Present

- 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
- The same problems apply for emerging networked computer systems (e.g., smartphones, IoT devices)

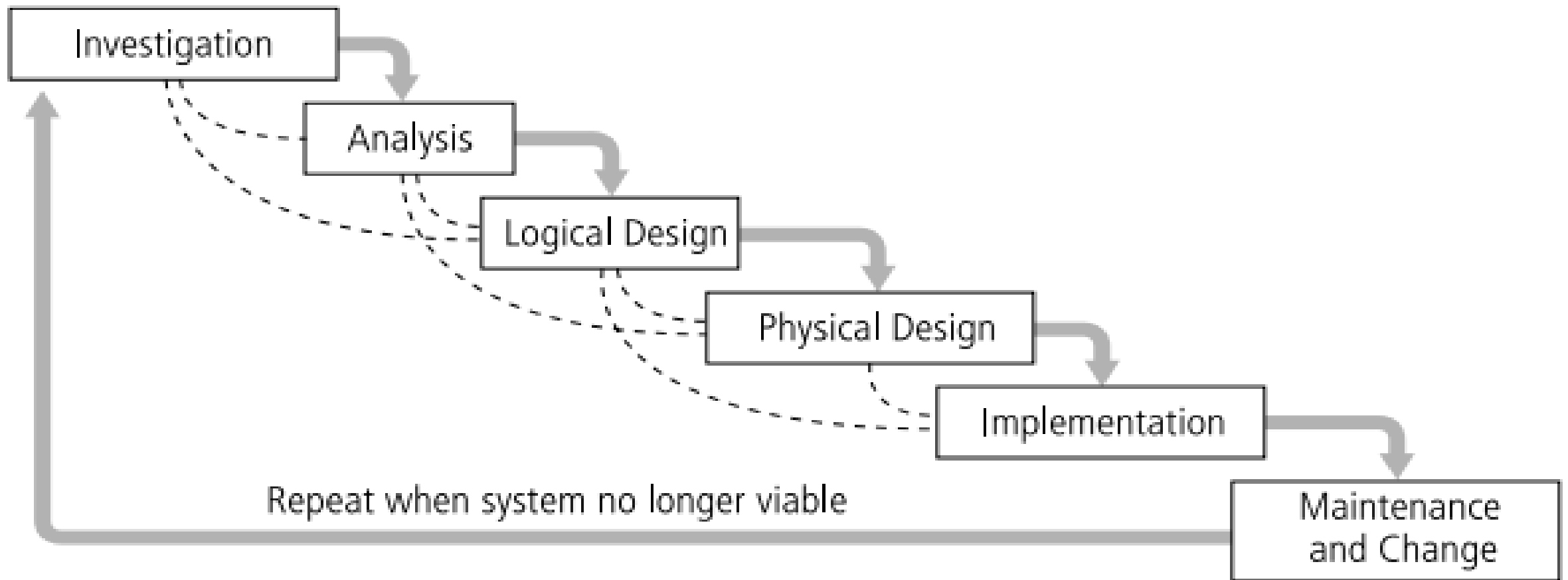
Top-down approach

Bottom-up approach

SDLC



SDLC Waterfall Methodology



The Security Systems Development Life Cycle

Phase 1: Investigation

- Outline project scope and goals
- Estimate costs
- Evaluate existing resources
- Analyze feasibility
- Management defines project processes and goals and documents these in the program security policy**

Phase 2: Analysis

- Assess current system against plan developed in Phase 1
- Develop preliminary system requirements
- Study integration of new system with existing system
- Document findings and update feasibility analysis
- Analyze existing security policies and programs
- Analyze current threats and controls
- Examine legal issues
- Perform risk analysis

Phase 3:

- Logical Design Assess current business needs against plan developed in Phase 2
- Select applications, data support, and structures
- Generate multiple solutions for consideration
- Document findings and update feasibility analysis
- Develop security blueprint
- Plan incident response actions
- Plan business response to disaster
- Determine feasibility of continuing and/or outsourcing the project

Phase 4 : Physical Design

- Select technologies to support solutions developed in Phase 3
- Select the best solution
- Decide to make or buy components
- Document findings and update feasibility analysis
- Select technologies needed to support security blueprint
- Develop definition of successful solution
- Design physical security measures to support technological solutions
- Review and approve project

Phase 5: Implementation

- Develop or buy software
- Order components
- Document the system
- Train users
- Update feasibility analysis
- Present system to users
- Test system and review performance
- Buy or develop security solutions
- At end of phase, present tested
- package to management for approval

Phase 6: Maintenance and Change

- Support and modify system during its useful life
- Test periodically for compliance with business needs
- Upgrade and patch as necessary
- Constantly monitor, test, modify, update, and repair to meet changing threats

The control and use of data in the organization is accomplished by

- Data owners—responsible for the security and use of a particular set of information
- Data custodians—responsible for the storage, maintenance, and protection of the information
- Data users—work with the information to perform their daily jobs supporting the mission of the organization

Summary

- Information security is a “well-informed sense of assurance that the information risks and controls are in balance.”
- Security should be considered a balance between protection and availability.
- Computer security began immediately after first mainframes were developed