# 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

# 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

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 1970s and 80s

- **ARPANET** was popular 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
- CREEPER, often referred to as the first computer virus was developed. This worm self-replicated as it traversed the ARPANET, a precursor to the Internet.

# The 1970s and 80s (continued)

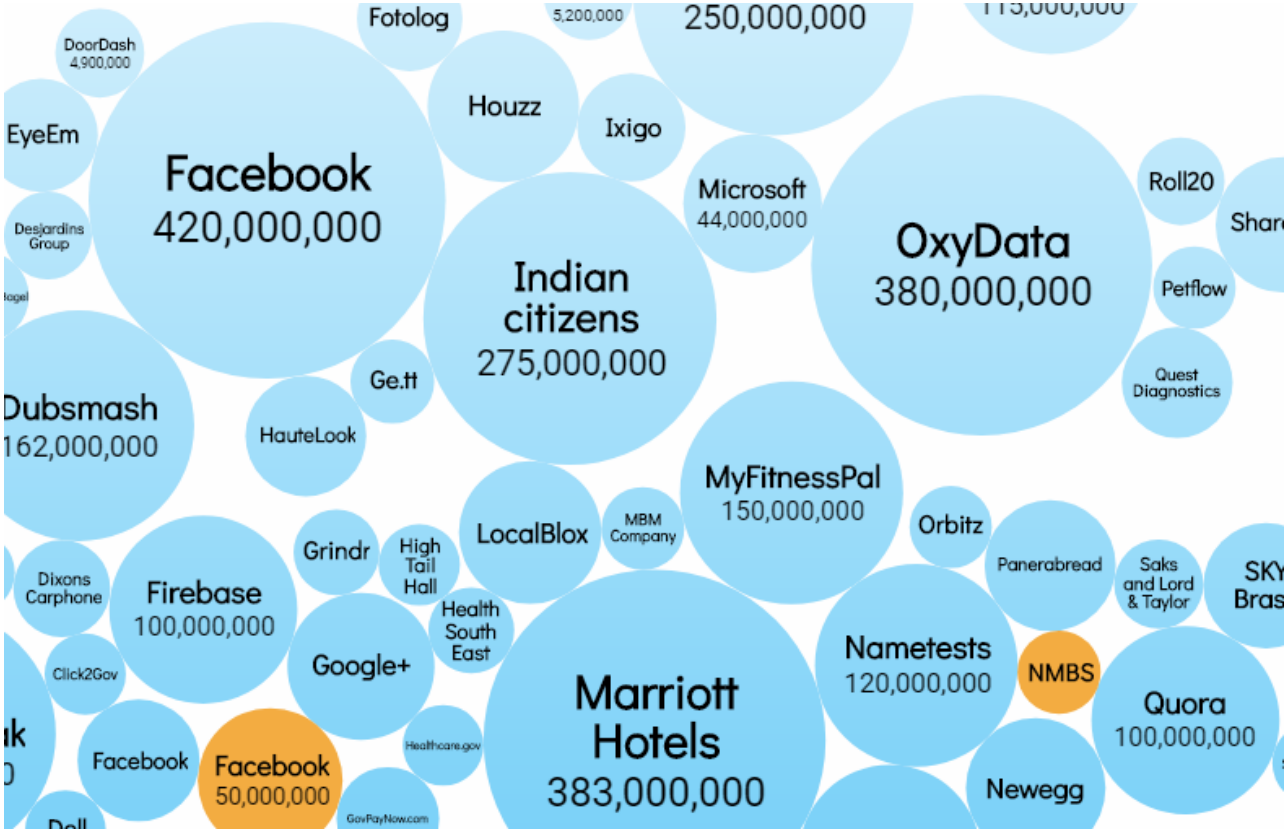
- Information security began with Rand Report R-609 (paper that started the study of computer security)
- Scope of computer security grew from physical security to include:
  - Safety of data
  - Limiting unauthorized access to data
  - Involvement of personnel from multiple levels of an organization
- 1980s - Morris Worm - The first virus distributed over the Internet resulted in the first felony conviction under the 1986 Computer Fraud and Misuse Act (CFAA).

# The 1990s

- Networks of computers became more common; so too did the need to interconnect networks
- 1990s - Firewalls - The first stateful filters and application layer firewalls emerge
- 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

# Previous breaches

- Go to https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

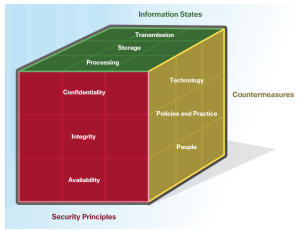


# What is Security?

- "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

The Infosecurity Cube

# The Three Dimensions




## The Principles of Security

- The first dimension of the Infosecurity cube identifies the goals to protect the Info world. The goals identified in the first dimension are the foundational principles of the Infosecurity world.
- These three principles are confidentiality, integrity and availability.
- The principles provide focus and enable the Info wizard to prioritize actions in protecting the Info world.
- Use the acronym CIA to remember these three principles.

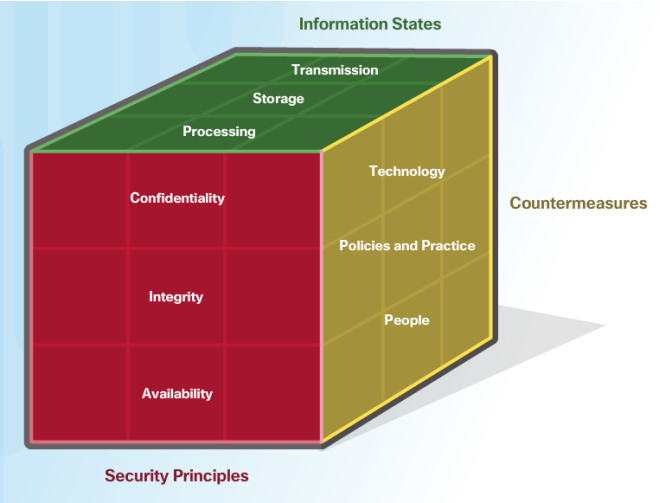

## The States of Data

- The Info world is a world of data; therefore, Info wizards focus on protecting data. The second dimension of the Infosecurity sorcery cube focuses on the problems of protecting all of the states of data in the Info world. Data has three possible states:

1) Data at rest or in storage 2) Data in transit 3) Data in process

# The Three Dimensions (Cont.)

## Infosecurity Safeguards




- The third dimension of the Infosecurity cube defines the types of powers used to protect the Info world. The sorcery cube identifies the three types of powers:
- **Technologies -** devices, and products available to protect information systems and fend off Info criminals.
- **Policies and Practices -** procedures, and guidelines that enable the citizens of the Info world to stay safe and follow good practices.
- **People -** Aware and knowledgeable about their world and the dangers that threaten their world.

CIA TRIAD

# Confidentiality

## The Principle of Confidentiality

- Confidentiality prevents the disclosure of information to unauthorized people, resources and processes. Another term for confidentiality is privacy.
- Organizations need to train employees about best practices in safeguarding sensitive information to protect themselves and the organization from attacks.
- Methods used to ensure confidentiality include data encryption, authentication, and access control.


## Protecting Data Privacy

- Organizations collect a large amount of data and much of this data is not sensitive because it is publicly available, like names and telephone numbers.
- Other data collected, though, is sensitive. Sensitive information is data protected from unauthorized access to safeguard an individual or an organization.

CIA TRIAD

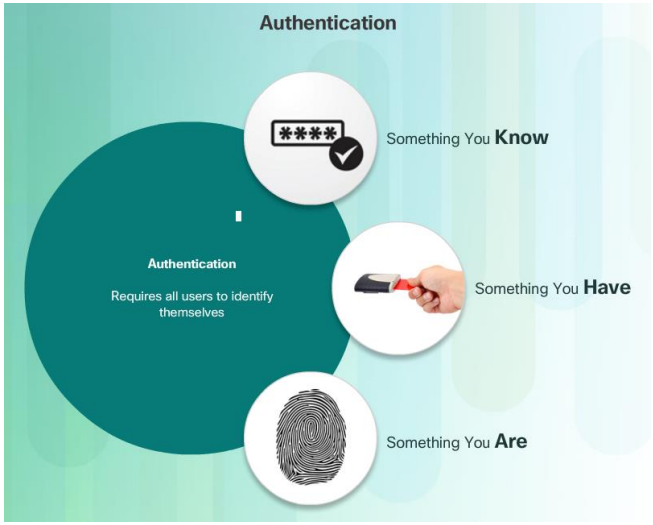
# Confidentiality (Cont.)

## Controlling Access

Access control defines a number of protection schemes that prevent unauthorized access to a computer, network, database, or other data resources. The concepts of AAA involve three security services: Authentication, Authorization and Accounting. ***Authentication*** verifies the identity of a user to prevent unauthorized access. Users prove their identity with a username or I.D.

***Authorization*** services determine which resources users can access, along with the operations that users can perform. Authorization can also control when a user has access to a specific resource.

***Accounting*** keeps track of what users do, including what they access, the amount of time they access resources, and any changes made.



CIA TRIAD

# Confidentiality (Cont.)

Confidentiality and privacy seem interchangeable, but from a legal standpoint, they mean different things.

- Most privacy data is confidential, but not all confidential data is private. Access to confidential information occurs after confirming proper authorization. Financial institutions, hospitals, medical professionals, law firms, and businesses handle confidential information.
- Confidential information has a non-public status. Maintaining confidentiality is more of an ethical duty.
- Privacy is the appropriate use of data. When organizations collect information provided by customers or employees, they should only use that data for its intended purpose.

**U.S. Laws**

- Privacy Act of 1974
- Freedom of Information ACT (FOIA)
- Family Education Records and Privacy Act (FERPA)
- U.S. Computer Fraud and Abuse Act (CFAA)
- U.S. Children's Online Privacy Protection Act (COPPA)
- Video Privacy Protection Act (VPPA)
- Health Insurance Portability & Accountability Act
- Gramm-Leach-Bliley Act (GLBA)
- California Senate Bill 1386 (SB 1386)
- U.S. Banking Rules and Regulations
- Payment Card Industry Data Security Standard (PCI DSS)
- Fair Credit Reporting Act (FCRA)

CIA TRIAD

# Integrity

## Principle of Data Integrity

- Integrity is the accuracy, consistency, and trustworthiness of data during its entire life cycle.
- Another term for integrity is quality.
- Methods used to ensure data integrity include hashing, data validation checks, data consistency checks, and access controls.

## Need for Data Integrity

- The need for data integrity varies based on how an organization uses data. For example, Facebook does not verify the data that a user posts in a profile.
- A bank or financial organization assigns a higher importance to data integrity than Facebook does. Transactions and customer accounts must be accurate.
- Protecting data integrity is a constant challenge for most organizations. Loss of data integrity can render entire data resources unreliable or unusable.

## Integrity Checks

- An integrity check is a way to measure the consistency of a collection of data (a file, a picture, or a record). The integrity check performs a process called a hash function to take a snapshot of data at an instant in time.

CIA TRIAD

# Availability

Data availability is the principle used to describe the need to maintain availability of information systems and services at all times. Infoattacks and system failures can prevent access to information systems and services.

- Methods used to ensure availability include system redundancy, system backups, increased system resiliency, equipment maintenance, up-to-date operating systems and software, and plans in place to recover quickly from unforeseen disasters.
- High availability systems typically include three design principles: eliminate single points of failure, provide for reliable crossover, and detect failures as they occur.

Organizations can ensure availability by implementing the following:

1. Equipment maintenance
2. OS and system updates
3. Test backups
4. Plan for disasters
5. Implement new technologies
6. Monitor unusual activity
7. Test to verify availability

States of Data

# Data at Rest

- Stored data refers to data at rest. Data at rest means that a type of storage device retains the data when no user or process is using it.
- A storage device can be local (on a computing device) or centralized (on the network). A number of options exist for storing data.
- Direct-attached storage (DAS) is storage connected to a computer. A hard drive or USB flash drive is an example of direct-attached storage.

States of Data

# Data at Rest (Cont.)

- Redundant array of independent disks (RAID) uses multiple hard drives in an array, which is a method of combining multiple disks so that the operating system sees them as a single disk. RAID provides improved performance and fault tolerance.
- A network attached storage (NAS) device is a storage device connected to a network that allows storage and retrieval of data from a centralized location by authorized network users. NAS devices are flexible and scalable, meaning administrators can increase the capacity as needed.
- A storage area network (SAN) architecture is a network-based storage system. SAN systems connect to the network using high-speed interfaces allowing improved performance and the ability to connect multiple servers to a centralized disk storage repository.

States of Data

# Data In Transit

Data transmission involves sending information from one device to another. There are numerous methods to transmit information between devices including:

- **Sneaker net** – uses removable media to physically move data from one computer to another
- **Wired networks** – uses cables to transmit data
- **Wireless networks** – uses the airwaves to transmit data

The protection of transmitted data is one of the most challenging jobs of a Infosecurity professional. The greatest challenges are:

- **Protecting data confidentiality** – Info criminals can capture, save and steal data in-transit.
- **Protecting data integrity** – Info criminals can intercept and alter data in-transit.
- **Protecting data availability** - Info criminals can use rogue or unauthorized devices to interrupt data availability.

States of Data

# Data In Process

The third state of data is data in process. This refers to data during initial input, modification, computation, or output.

- Protection of data integrity starts with the initial input of data.
- Organizations use several methods to collect data, such as manual data entry, scanning forms, file uploads, and data collected from sensors.
- Each of these methods pose potential threats to data integrity.
- Data modification refers to any changes to the original data such as users manually modifying data, programs processing and changing data, and equipment failing resulting in data modification.
- Processes like encoding/decoding, compression/decompression and encryption/decryption are all examples of data modification. Malicious code also results in data corruption.

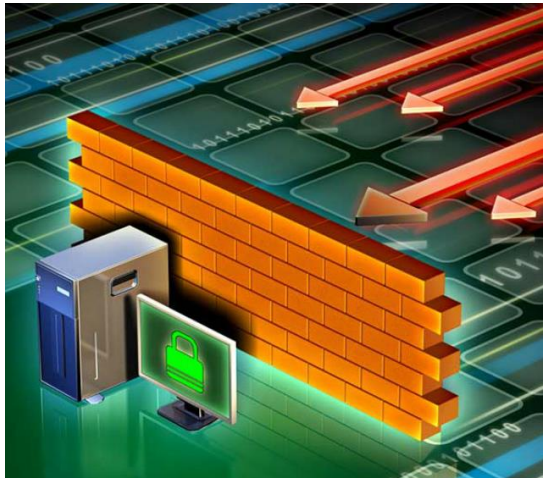
# Technologies

## Software-based Technology Safeguards

- Software safeguards include programs and services that protect operating systems, databases, and other services operating on workstations, portable devices, and servers. There are several software-based technologies used to safeguard an organization's assets.

## Hardware-based Technology Safeguards

- Hardware based technologies are appliances that are installed within the network faculties. They can include: Firewall appliances, Intrusion Detection Systems (IDS),Intrusion Prevention Systems (IPS) and Content filtering systems.



# Technologies

## Network-based Technology Safeguards

Technological countermeasures can also include network-based technologies.


- **Virtual Private Network (VPN)** is a secure virtual network that uses the public network (i.e., the Internet). The security of a VPN lies in the encryption of packet content between the endpoints that define the VPN.
- **Network access control (NAC)** requires a set of checks before allowing a device to connect to a network. Some common checks include up-to-data antivirus software or operating system updates installed.
- **Wireless access point security** includes the implementation of authentication and encryption.

# Technologies

## Cloud-based Technology Safeguards

- Technological countermeasures now also include cloud-based technologies. Cloud-based technologies shift the technology component from the organization to the cloud provider.
- **Software as a Service (SaaS)** allows users to gain access to application software and databases. Cloud providers manage the infrastructure. Users store data on the cloud provider's servers.
- **Infrastructure as a Service (IaaS)** provides virtualized computing resources over the Internet. The provider hosts the hardware, software, servers, and storage components.
- **Virtual security appliances** run inside a virtual environment with a pre-packaged, hardened operating system running on virtualized hardware.

# Implementing Infosecurity Education and Training

A security awareness program is extremely important for an organization. An employee may not be purposefully malicious but just unaware of what the proper procedures are.

There are several ways to implement a formal training program:

- Make security awareness training a part of the employee's onboarding process
- Tie security awareness to job requirements or performance evaluations
- Conduct in-person training sessions
- Complete online courses

Security awareness should be an ongoing process since new threats and techniques are always on the horizon.

# Infosecurity Policies and Procedures

- A security **policy** is a set of security objectives for a company that includes rules of behavior for users and administrators and specifies system requirements. These objectives, rules, and requirements collectively ensure the security of a network, the data, and the computer systems within an organization.
- **Standards** help an IT staff maintain consistency in operating the network. Standards provide the technologies that specific users or programs need in addition to any program requirements or criteria that an organization must follow.
- **Guidelines** are a list of suggestions on how to do things more efficiently and securely. They are similar to standards, but are more flexible and are not usually mandatory. Guidelines define how standards are developed and guarantee adherence to general security policies.
- **Procedure** documents are longer and more detailed than standards and guidelines. Procedure documents include implementation details that usually contain step-by-step instructions and graphics.

# 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

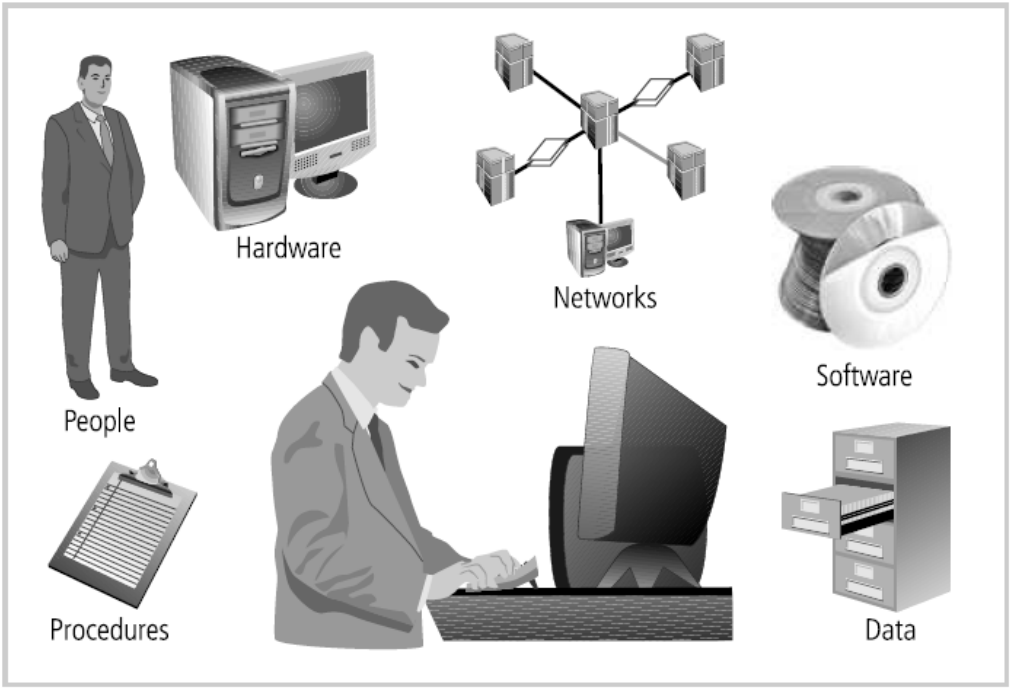



**Figure 1-7** Components of an Information System

# 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

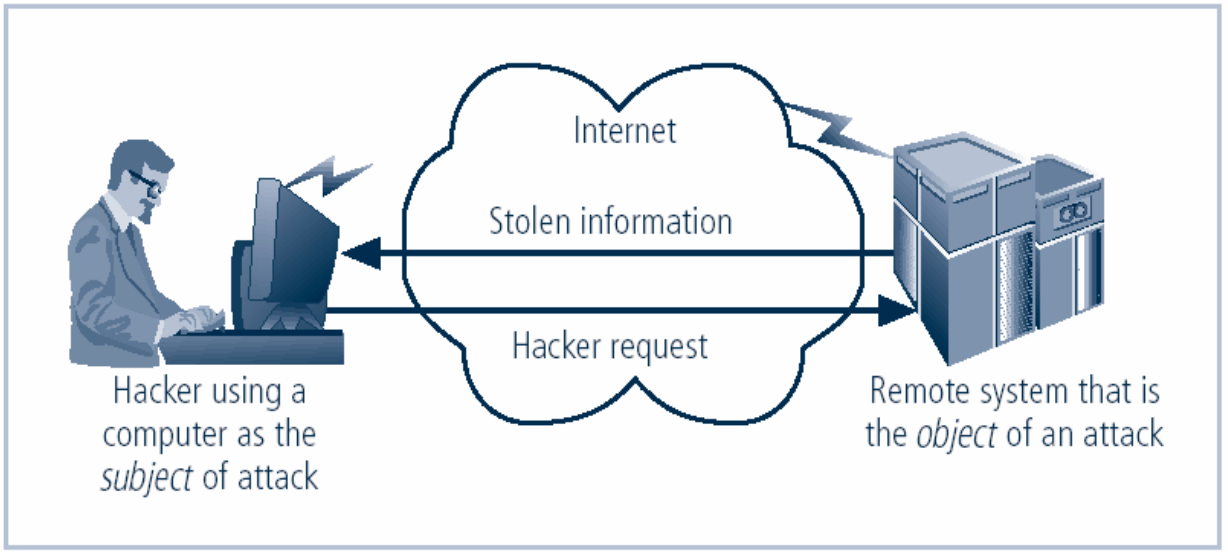



**FIGURE 1-6** Computer as the Subject and Object of an Attack

# 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

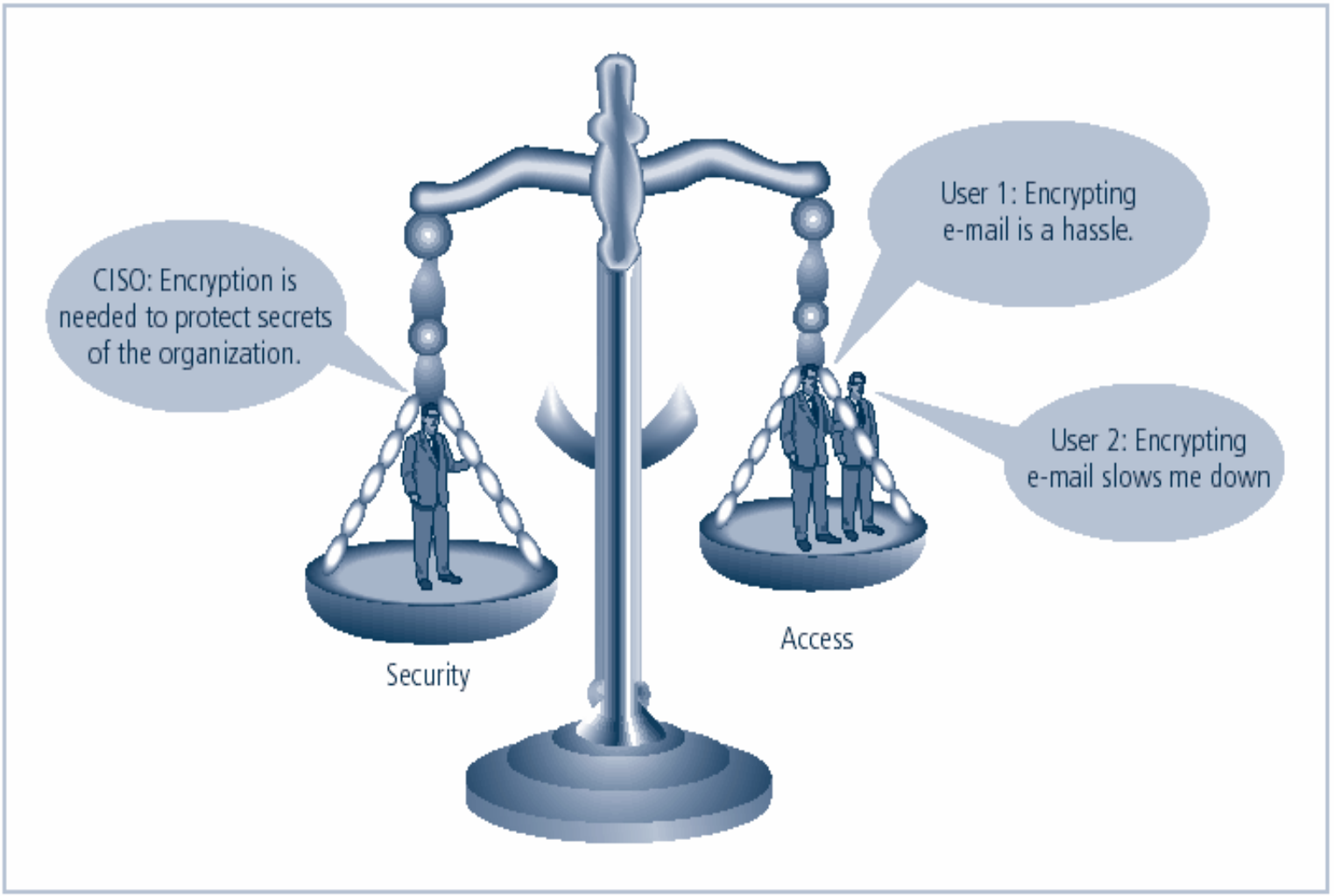



**FIGURE 1-7** Balancing Information Security and Access

# 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

# 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

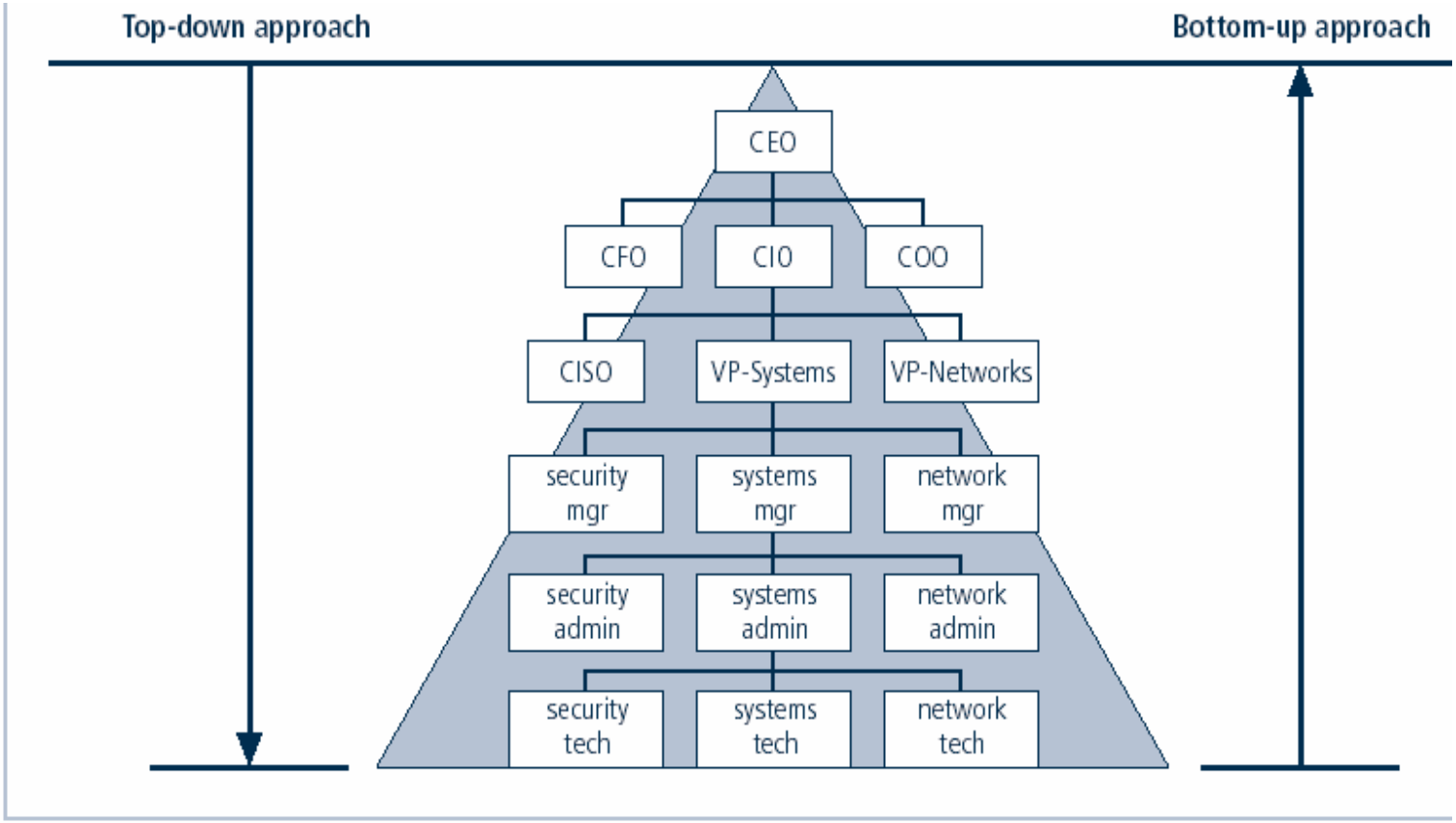



**FIGURE 1-8** Approaches to Information Security Implementation

# 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 (continued)

- Security should be considered a balance between protection and availability
- Information security must be managed similarly 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