Introduction

Information Security (CSC-407)

Fall 2024 (BSE-7A & 7B)

Information Asset

- An **asset** is anything of value.
- **Digital information** is an asset that has a value, hence it needs to be secured from attacks.
- Professional practitioners recognize that ***information security*** needs to be aligning with ***business objectives***.
- Not only should information be secured when **stored in computers**, there should also be ways to maintain security when **processed** or **transmitted**.

Information Security

- **Security:** is protection from adversaries, who would do harm, ***intentionally*** or ***un-intentionally***.
- **Information security:** Protection of ***confidentiality***, ***integrity***, and ***availability*** of "information assets" whether in ***storage, processing or transmission***, via the application of ***policy, education, training, awareness*** and ***technology***.
- **EC-COUNCIL Information security:** the state of the well-being of **information** and **infrastructure** in which possibility of theft, tampering, or disruption of information and services is **kept low** or **tolerable**.

Cyber Security Incidents

- 2024, **faulty software update** for Microsoft Windows by cybersecurity firm CrowdStrike caused a global IT outage. Disrupted airline and hospital operations, affected 8.5 million machines, cost 500 companies **$5.4 billion**.
- 2023, Israeli-linked hackers disrupted 70% of gas stations in Iran. **Pumps** restored operation next day, but payment issues carried for several days.
- 2022, a **DDoS attack** knocked websites belonging to Ukrainian Defense Ministry and two of country's largest banks offline.

Cyber Security Incidents (Cont.)

- 2020, Amazon experienced 2.3Tbps **DDoS attack** as being the largest ever recorded DDoS attack in history.
- 2016, Uber data of 57 million users and 600,000 drivers **exposed**.
- 2015, Ukraine **Power Grid**, 30 substations switched off and about 230,000 people left without electricity for 1 ~ 6 hours.

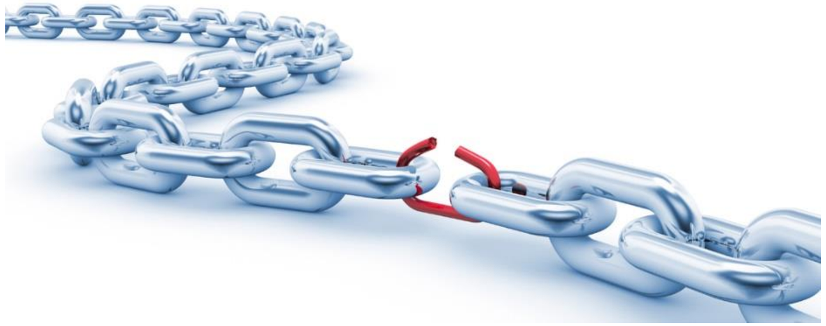
Significant Cyber Incidents Since 2006:
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Software Defect Incident

- US Northeast blackout (2003): ***Not a Cyber Attack!***
  - **Cause:** a software defect in a control room.
  - **Restoration:** some customers after 6 hours, some after 2 days, some remote places after nearly a week.
  - **Consequences (among other):**
    - 45M people in 8 US states
    - 10M people in Canada
    - Healthcare facilities experienced $100M lost revenue
    - 6 hospitals bankrupt one year after

Key Terminologies

- The term security is used in the sense of minimizing the vulnerabilities of assets and resources.
- **Vulnerability:** any weakness that could be **exploited** to violate a system or the information it contains.



Key Terminologies (Cont.)

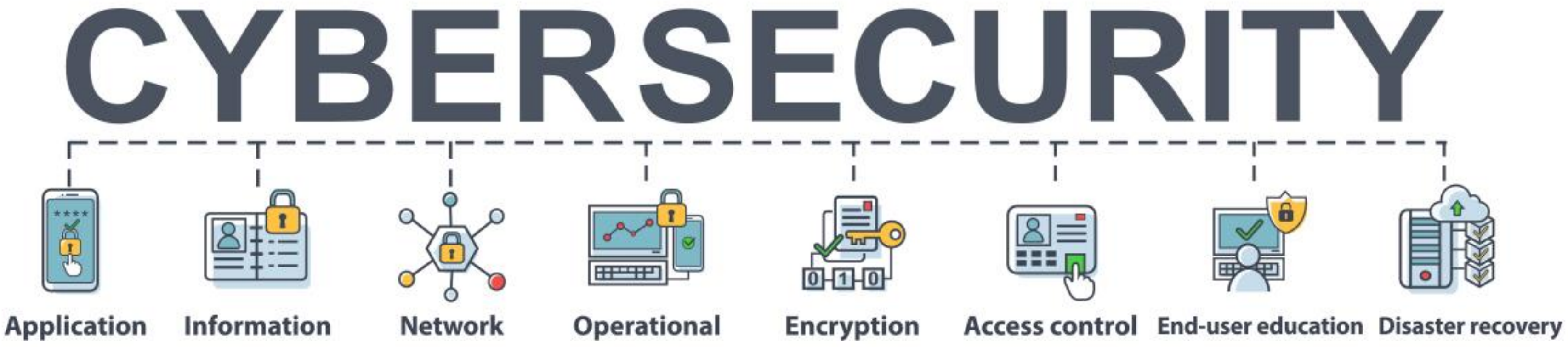
- **Computer Security:** the protection to an automated information system for preserving the **confidentiality, integrity**, and **availability** of information system resources.

Key Terminologies (Cont.)

- **Network and Internet Security:** measures to detect, deter and correct security violations that involve the transmission of information.

Key Terminologies (Cont.)

- **Cybersecurity:** the protection of **digital information** and **IT infrastructure**, including computers, servers, networks and devices from cyber-attacks.



Need for Security

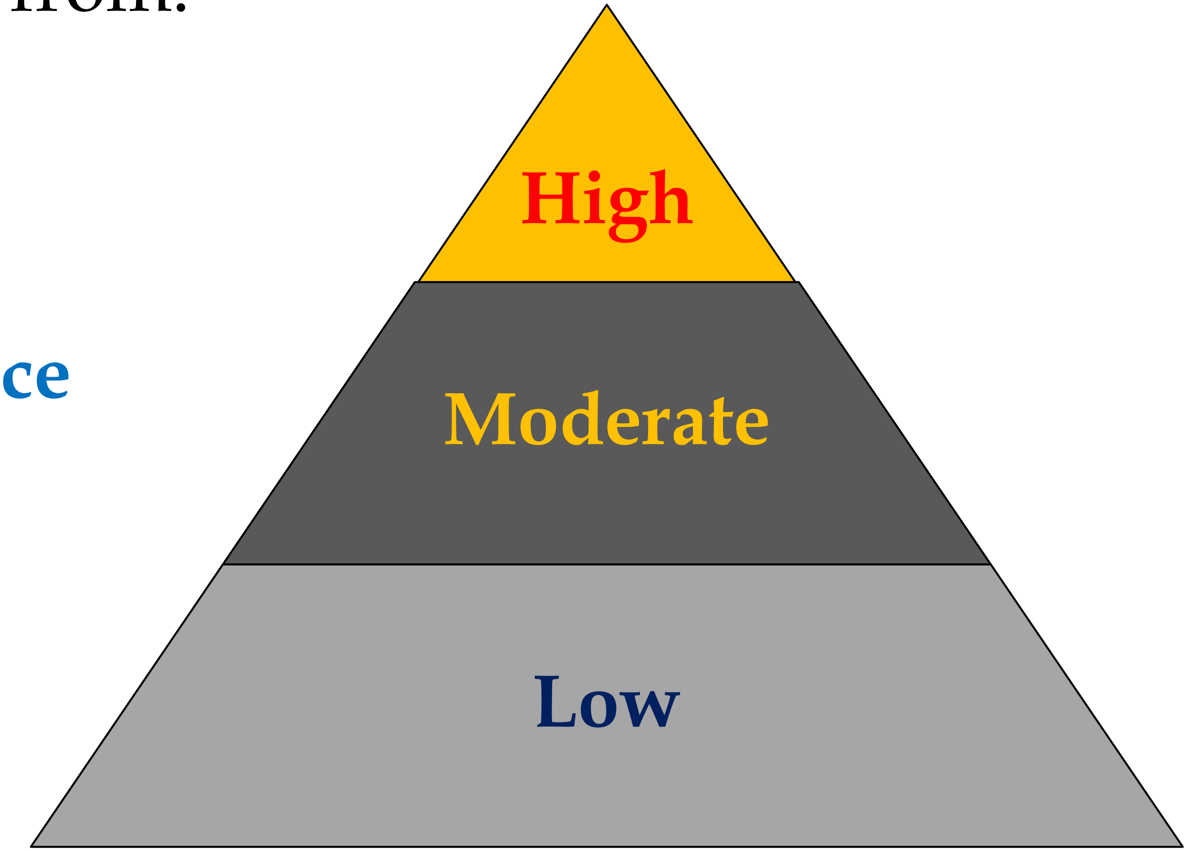
There is a growing need for security due to:

1. **Evolution** of technology
2. Rely on **computers** for many things
3. Increased **network** environment
4. Increasing **complexity** of computer based systems
5. Direct **impact** of security breach on the victims

Impact of Security Breaches

Impact of security breaches varies from:

1. **Reputation** damage
2. Weakening **customer loyalty**
3. Diminishing **investor confidence**
4. **Monetary** loss
5. **Legal** consequences



Business Needs for Security

1. **Protecting Functionality;** ***General management, IT management and IS management*** are each responsible for facilitating security to protect organization ability to function.
2. **Protecting Data;**
   - **Data security** is a critical aspect of IS, where the value of data motivates attackers to steal, sabotage or corrupt it.
   - An **effective IS program** protects organization's data.
   - Maintaining the confidentiality, integrity and availability of data managed by a **DBMS** is known as **database security**.

Business Needs for Security (Cont.)

2. Protecting Data (Cont.);

- Database security is accomplished by applying a broad range of **control approaches**, including:
  - **Managerial controls:** policy, procedure, and governance.
  - **Physical controls** data centers with locking doors, fire suppression systems, video monitoring and security guards.
  - **Technical controls:** access control, authentication, auditing, backup, recovery, encryption and integrity controls.

Business Needs for Security (Cont.)

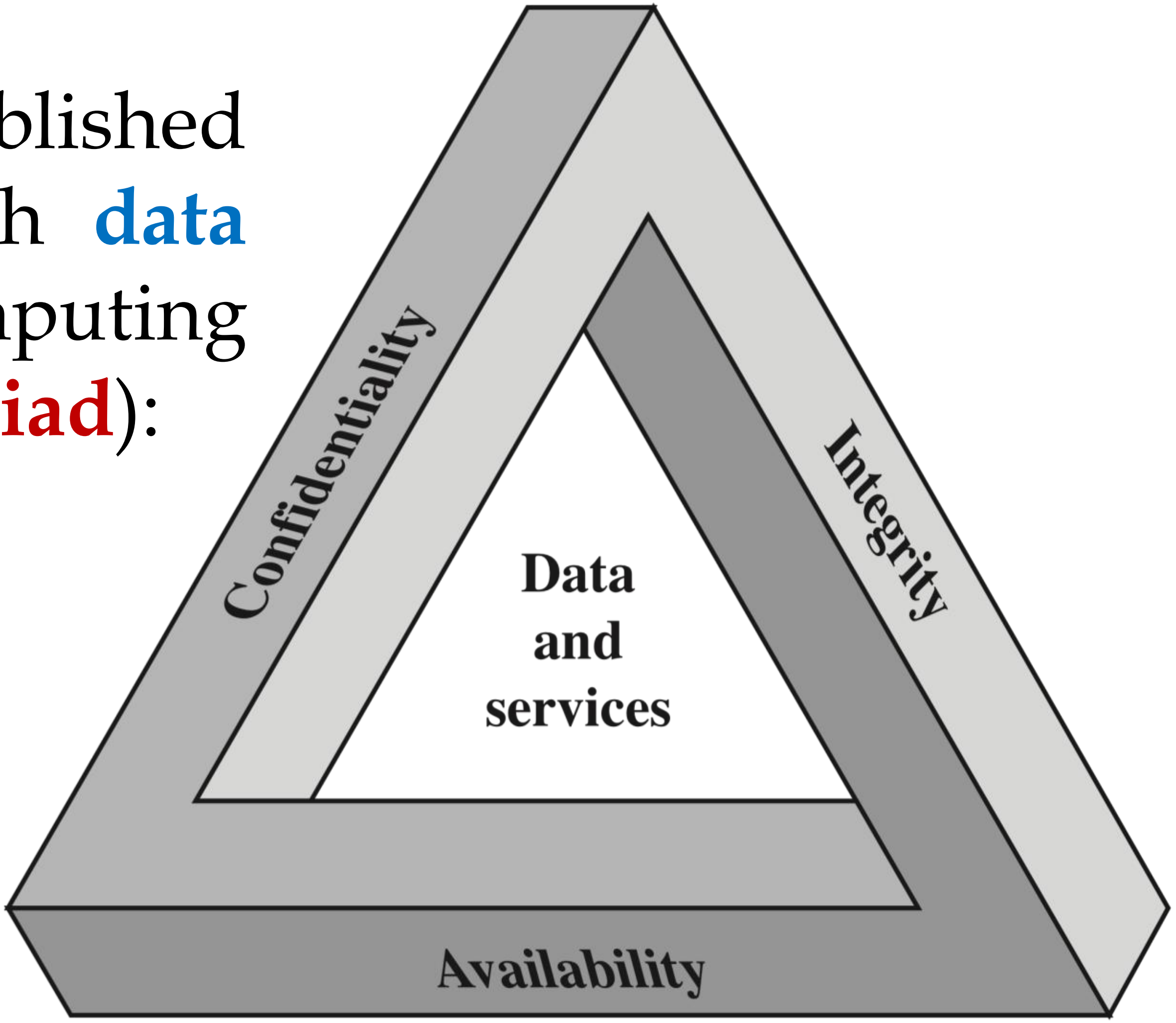
3. Enabling Safe Operation of Applications;

- Organizations are under immense pressure to operate **diversified set of applications**.
- Modern organization needs to create an environment that safeguards these applications, especially those that are important elements of organization's infrastructure ***(e.g. OS, operational applications, E-mail and IM applications)***.

Security Goals

- There are three well-established major security goals for both **data** and for information and computing **services** (referred to as **CIA Triad**):

1. **Confidentiality**
2. **Integrity**
3. **Availability**



Security Goals (Cont.)

- **Confidentiality:** maintaining authorized restrictions on information access and disclosure.
- **Integrity:** guarding against improper information modification or destruction, including ensuring information **nonrepudiation** and **authenticity**.
- **Availability:** ensuring timely and reliable access to entities when needed.

Security Goals (Cont.)

- Additional requirements for security goals are:

1. **Authenticity:** the property of being genuine and to be verified and trusted; hence confidence in the validity of a transmission, a message, or message originator.

2. **Accountability:** the requirement for actions so an entity can be uniquely traceable.

Nonrepudiation!

- Prevents either sender or receiver from **denying** a transmitted message.
  - When a message is sent, the receiver can prove that the alleged sender in fact sent the message.
  - When a message is received, the sender can prove that the alleged receiver in fact received the message.

Security Threats & Attacks

- **Threat:** a possible danger that might exploit a vulnerability resulting into a **breach** in security and causing harm.

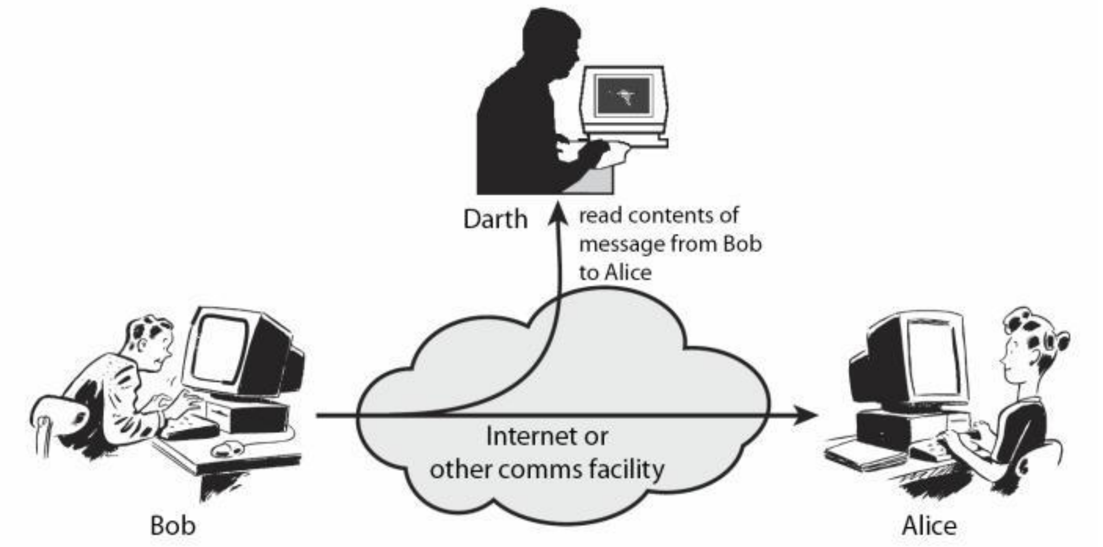
- **Security attack:** “an assault” on system security that derives from an intelligent threat, which is a deliberate attempt to evade security services and violate the security policy of a system.

- Ways of classifying security attacks:

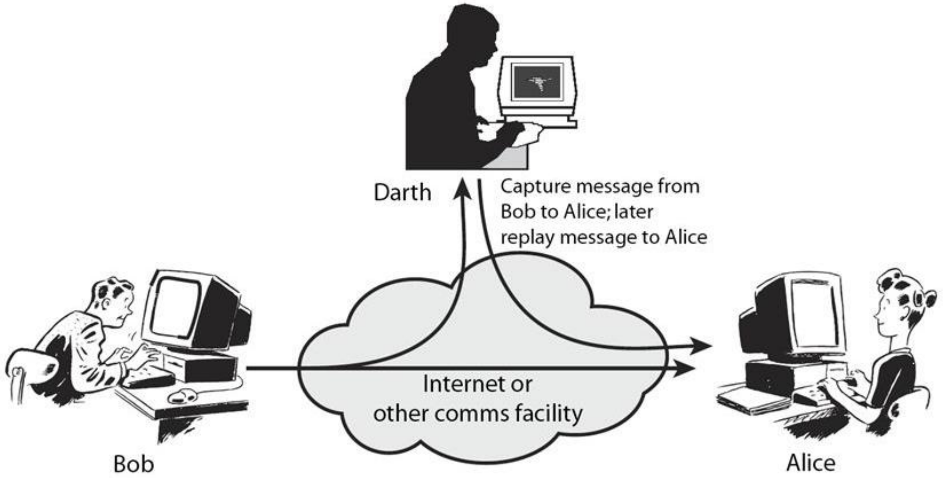
Method 1	Method 2
Passive attacks	Direct
Active attacks	Indirect

Passive & Active Attacks

- **Passive attack:** an attack that attempts to learn or make use of information from the system but does not affect system resources.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

- **Active attack:** an attack that attempts to alter system resources or affect their operation.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Passive Attack

- Passive attack (Sometimes referred to as **"tapping or snooping"**) are in the nature of **eavesdropping** on transmissions.
- In passive attack, the attacker cannot interact with any of the parties involved.
- Attacker attempts to obtain information transmitted, sometimes by ***traffic analysis*** and may lead to ***release of message contents***.

Passive Attack (Cont.)

- **Q) Passive attacks are very difficult to detect, why?**
- A) Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. Hence, passive attacks do not involve any alteration of data, making it difficult to detect.
- **Solution:**

  It is feasible to prevent the success of such attacks, usually by means of **encryption**. Thus, the emphasis in dealing with passive attacks is on ***prevention rather than detection***.

Active Attack

- Active attacks involve some modification of data stream or creation of a false stream.
- Active attacks can be subdivided into four types:
  - Masquerade *(also know as **spoofing**)*
  - Replay
  - Modification
  - Denial of service (DoS)

Active Attack (Cont.)

1. **Masquerade** or **spoofing** takes place when an attacker **impersonates** someone else.
2. **Replay** involves the passive capture of a data unit and its subsequent **retransmission** to produce an unauthorized effect.
3. **Modification** means that some portion of a legitimate message is **altered**, or that message is delayed or reordered, to produce an unauthorized effect.
4. **Denial of service prevents** the normal use of a system by slowing them down or totally interrupting the service.

Active Attack (Cont.)

- **Q) It is difficult to prevent active attacks absolutely, why?**
- A) Because of the wide variety of potential physical, software, and network vulnerabilities.
- **Solution:**
- The goal is to detect active attacks and to recover from any disruption caused by them. If the detection has a deterrent effect, it may also contribute to prevention.

Passive & Active Attacks on CIA Triad

Taxonomy of Attacks with Relation to Security Goals

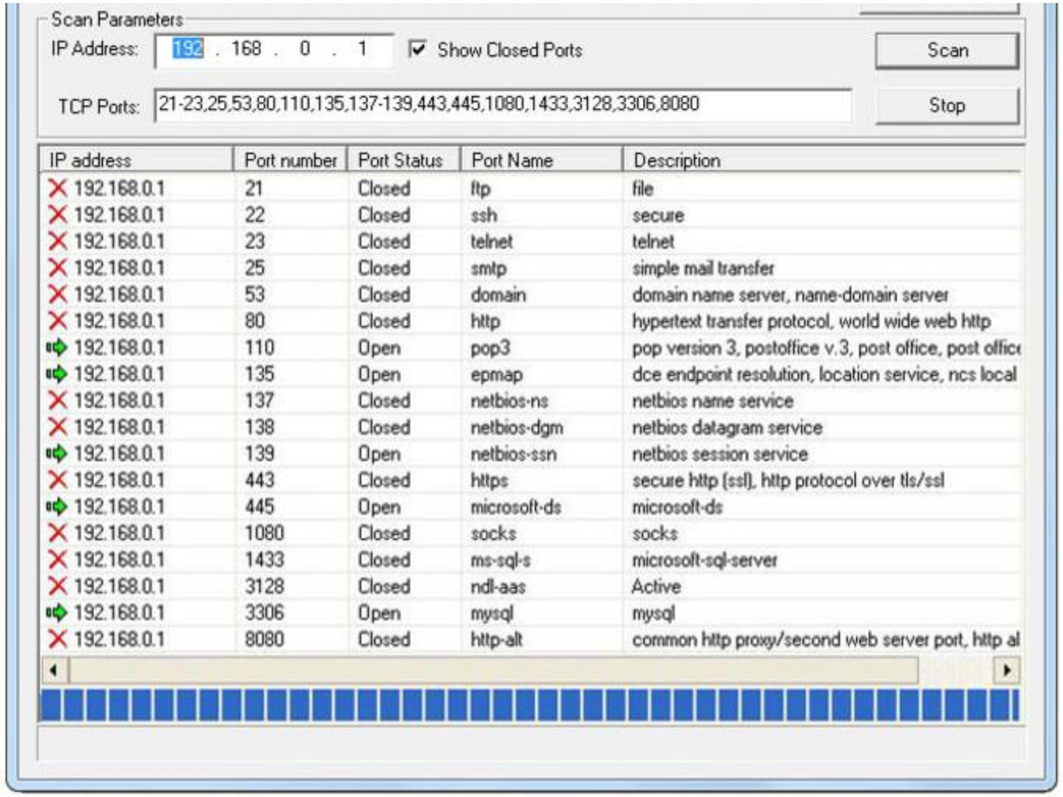
Attacks	Passive/ Active	Threatening to CIA Triad
Snooping	Passive	Confidentiality
Traffic analysis		
Modification	Active	Integrity
Masquerading		
Replaying		
Denial of service	Active	Availability

Direct & Indirect Attacks

- **Direct attack:** an attack committed directly by a hacker using a PC to break into a system.
- **Indirect attack:** an attack committed by a hacker through compromising a system and using it to attack other systems ***(e.g. through botnets)***.

Attack Surfaces

- **Attack surface:** the sum of the different points that are reachable and exploitable vulnerabilities in a system.
- **Examples:** ***open ports, SQL injection in web forms, code that processes incoming data and social engineering.***



Scan Parameters

IP Address: 192 . 168 . 0 . 1 ☑ Show Closed Ports

TCP Ports: 21-23,25,53,80,110,135,137-139,443,445,1080,1433,3128,3306,8080

IP address	Port number	Port Status	Port Name	Description
✗ 192.168.0.1	21	Closed	ftp	file
✗ 192.168.0.1	22	Closed	ssh	secure
✗ 192.168.0.1	23	Closed	telnet	telnet
✗ 192.168.0.1	25	Closed	smtp	simple mail transfer
✗ 192.168.0.1	53	Closed	domain	domain name server, name-domain server
✗ 192.168.0.1	80	Closed	http	hypertext transfer protocol, world wide web http
➡ 192.168.0.1	110	Open	pop3	pop version 3, postoffice v.3, post office, post offic
➡ 192.168.0.1	135	Open	epmap	dce endpoint resolution, location service, ncs local
✗ 192.168.0.1	137	Closed	netbios-ns	netbios name service
✗ 192.168.0.1	138	Closed	netbios-dgm	netbios datagram service
➡ 192.168.0.1	139	Open	netbios-ssn	netbios session service
✗ 192.168.0.1	443	Closed	https	secure http (ssl), http protocol over tls/ssl
➡ 192.168.0.1	445	Open	microsoft-ds	microsoft-ds
✗ 192.168.0.1	1080	Closed	socks	socks
✗ 192.168.0.1	1433	Closed	ms-sql-s	microsoft-sql-server
✗ 192.168.0.1	3128	Closed	ndl-aas	Active
➡ 192.168.0.1	3306	Open	mysql	mysql
✗ 192.168.0.1	8080	Closed	http-alt	common http proxy/second web server port, http al

Attack Surfaces (Cont.)

Benefits of Attack Surface Analysis:

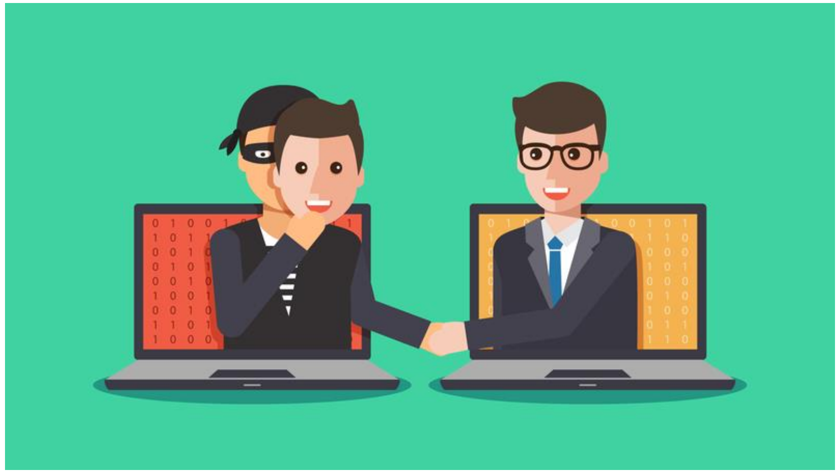
1. Assessing **scale** and **severity** of **threats** to a system.
2. Makes **developers** and **security analysts** aware of *"where"* **security mechanisms** are required.
3. Provides guidance on **setting priorities** for testing, strengthening security and modifying services or applications.
4. Designers may be able to find ways to ***make the attack surface smaller***, hence ***making the task of attacker more difficult***.

Attack Surfaces Categories

- **Network attack surface** refers to vulnerabilities over a network, including network protocol vulnerabilities, disruption of communications links and various forms of intruder attacks.
- **Software attack surface** refers to vulnerabilities in application, utility or operating system code. A particular focus in this category is **Web server software**.
- **Human attack surface** refers to vulnerabilities created by personnel or outsiders, such as **social engineering**, **human error** and **trusted insiders.**

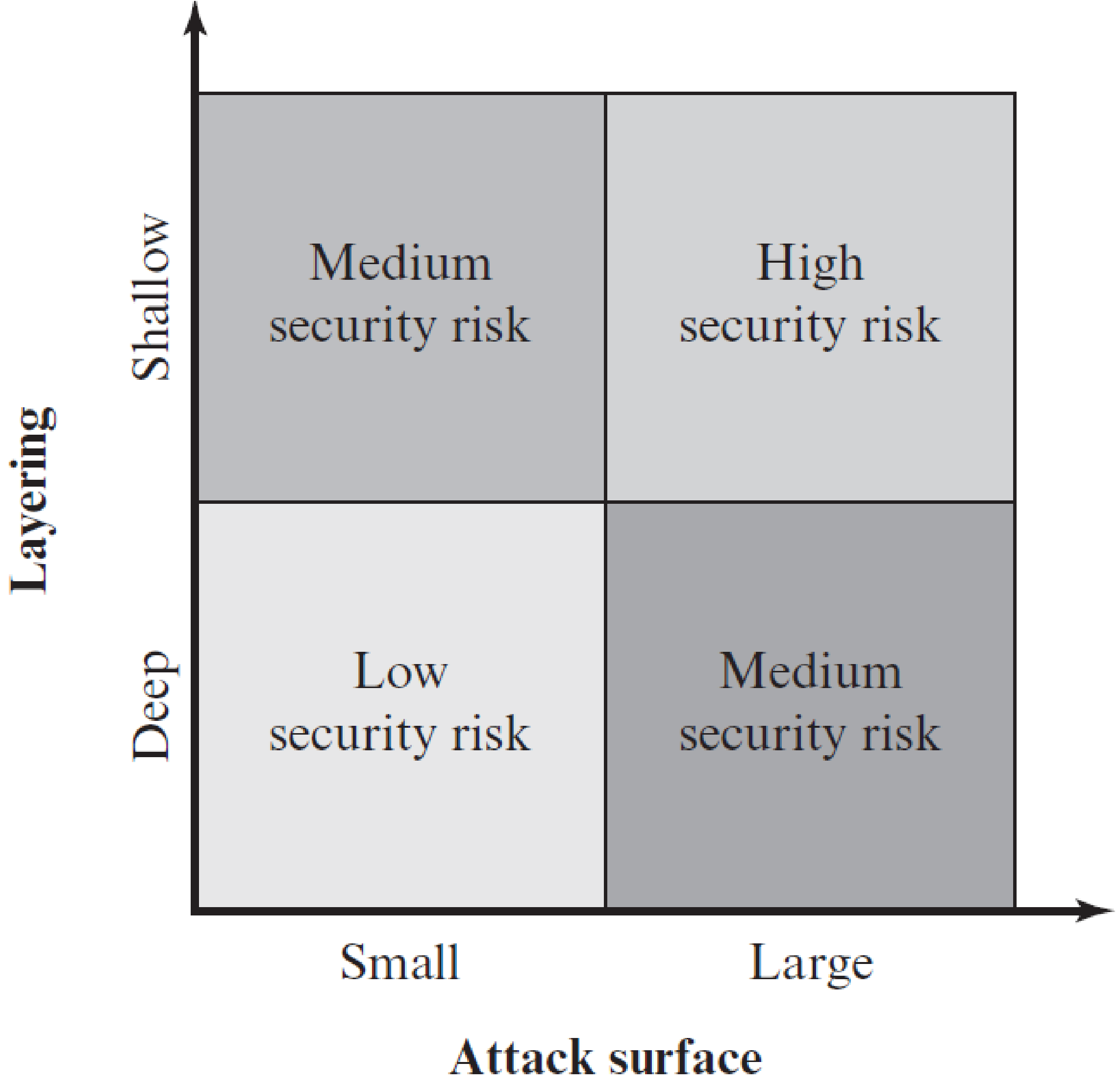
Attack Surfaces Categories (Cont.)

- Nowadays, attacks are not getting into networks only through vulnerabilities in **network** and **software** services.
- In-fact, recent statistics show that **80-90%** of attacks use **social engineering**.



Defense-in-Depth

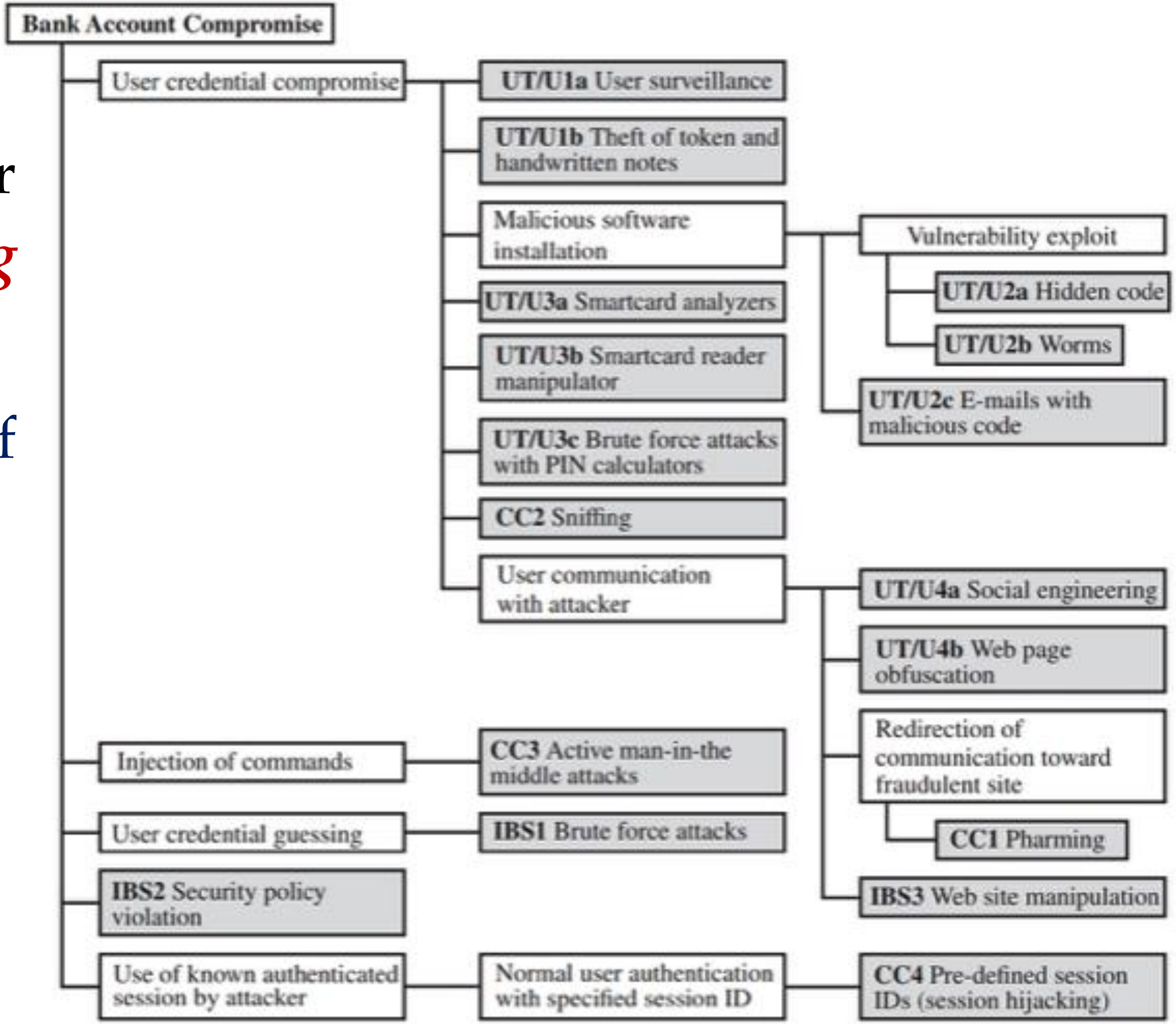
- Keeping the **attack surface** as small as possible is a basic security measure.
- Use of **layering** ***(i.e. defense in depth)*** with reduction of attack surface complements each other in mitigating security risk.



Attack Trees

- **Attack tree:** a **hierarchical structure** that represents a ***set of potential techniques*** for exploiting security vulnerabilities.
- The **security incident** ***(i.e. the attack goal)*** is represented as the **root node** of the tree while the ways an attacker could reach that goal are incrementally represented as **branches** and **sub-nodes**.
- Each **sub-node** defines a **sub-goal**, and each **sub-goal** may have its own set of further **sub-goals**, and so on.
- The different ways to **initiate** an attack is through **leaf nodes**.

- Attack Tree analysis for ***Internet Banking Authentication***.
- Shaded boxes are leaf nodes.



- Bank Account Compromise
  - User credential compromise
    - UT/U1a User surveillance
    - UT/U1b Theft of token and handwritten notes
    - Malicious software installation
      - Vulnerability exploit
        - UT/U2a Hidden code
        - UT/U2b Worms
      - UT/U2c E-mails with malicious code
    - UT/U3a Smartcard analyzers
    - UT/U3b Smartcard reader manipulator
    - UT/U3c Brute force attacks with PIN calculators
    - CC2 Sniffing
    - User communication with attacker
      - UT/U4a Social engineering
      - UT/U4b Web page obfuscation
      - Redirection of communication toward fraudulent site
        - CC1 Pharming
      - IBS3 Web site manipulation
  - Injection of commands
    - CC3 Active man-in-the middle attacks
  - User credential guessing
    - IBS1 Brute force attacks
  - IBS2 Security policy violation
  - Use of known authenticated session by attacker
    - Normal user authentication with specified session ID
      - CC4 Pre-defined session IDs (session hijacking)

Attack Trees (Cont.)

Benefits of Attack Trees:

1. Effectively use the information on **attack patterns**.
2. The attack tree can guide both the **design of systems** and **applications**, along with choice and strength of countermeasures.
3. **Security analysts** can use the attack tree to **document security attacks** in a structured form that reveals key vulnerabilities.

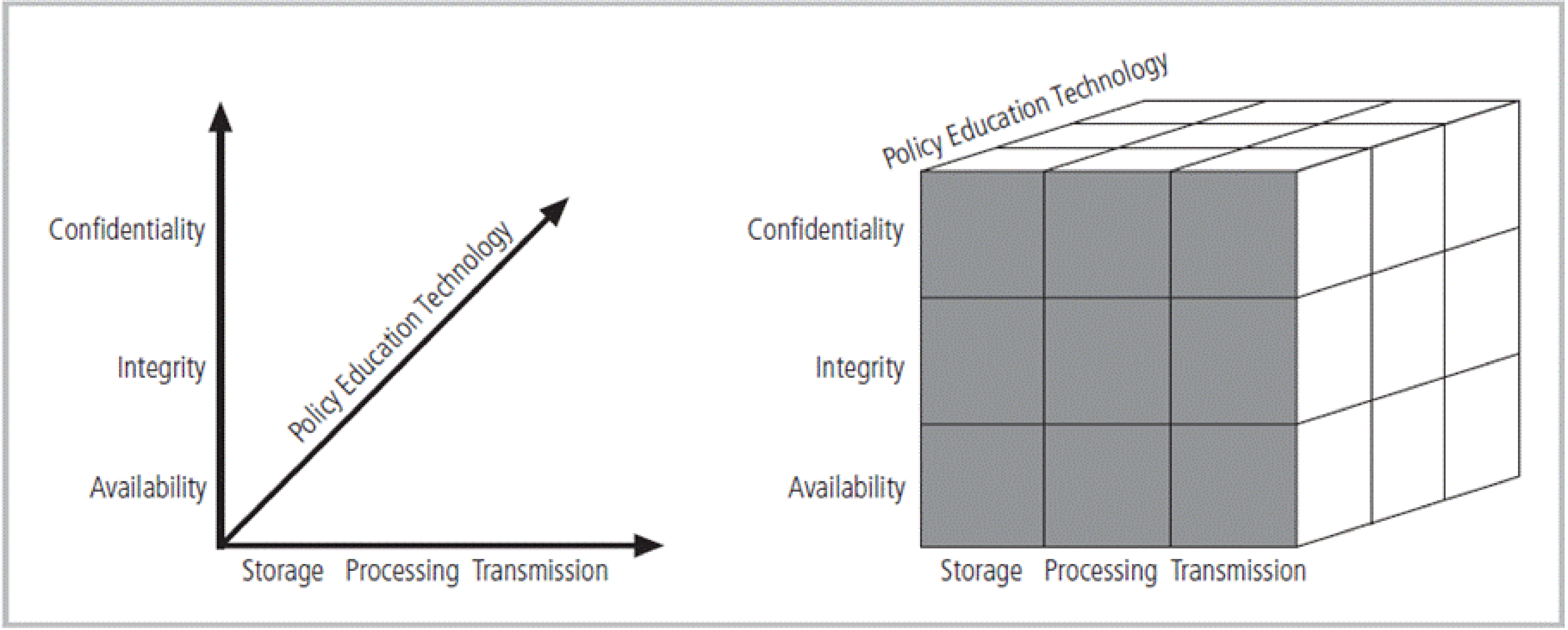
CNSS Security Model

- **McCumber Cube** is a graphical representation of the different approaches for computer and information security.

- ***McCumber Cube*** shows three dimensions, composed of **3×3×3**, i.e. **27 cells** representing areas that must be addressed to secure today's information systems.

- To ensure comprehensive system security, **each of the 27 areas** must be properly addressed during the security process.

CNSS Security Model (Cont.)


Confidentiality
Integrity
Availability
Policy Education Technology
Storage Processing Transmission
Policy Education Technology
Confidentiality
Integrity
Availability
Storage Processing Transmission

CNSS Security Model (Cont.)

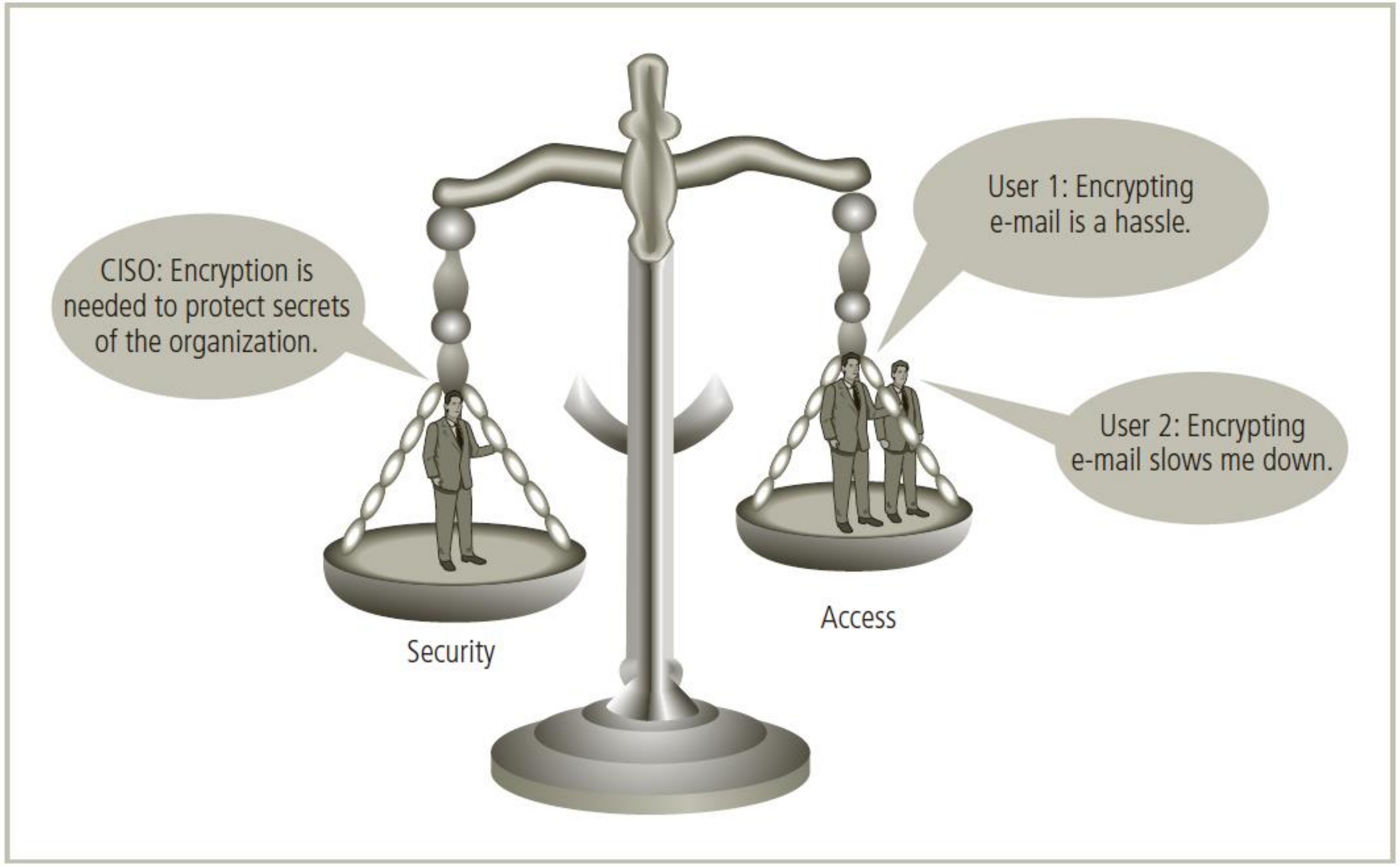
- E.g., the intersection of ***"technology, integrity and storage"*** requires a set of controls though technology to protect integrity of information while in storage.
- One such control is the ***Intrusion Detection System (IDS)*** for detecting host intrusion that protects **integrity** of information by alerting security administrators to potential **modification of a critical file**.

Balancing IS and Access

- Even with the best planning and implementation, it is **impossible** to obtain **perfect information security**.
- A system can be made available to anyone, anywhere, anytime, through any means. However, such **unrestricted access** poses a danger to the security of information.
- On the other hand, a completely secure information system would not allow **anyone access**.

Balancing IS and Access (Cont.)

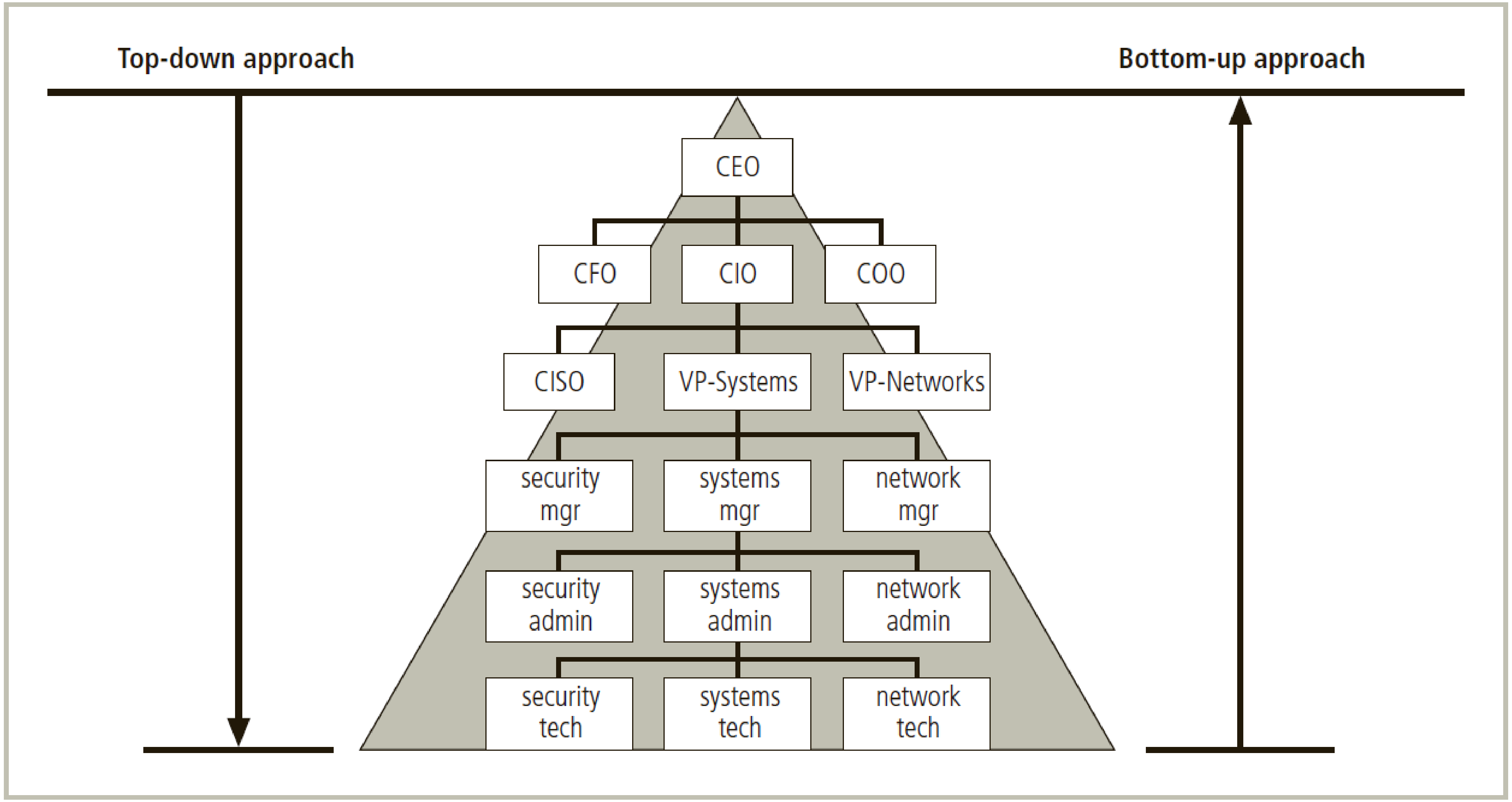
- To achieve balance, ***i.e. to operate an information system that satisfies the user and security professional***, the security level must allow **reasonable access** yet protect against threats.


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

IS Implementation Approaches

- The implementation of information security in an organization must begin somewhere and ***cannot happen overnight***.
- Securing information assets is an **incremental process** that requires coordination, time and patience.
- Two key approaches of IS implementation include:
  - ➢ **Bottom-up approach**
  - ➢ **Top-down approach**

Bottom-up & Top-down Approaches



Bottom-up Approach

- In bottom-up approach, information security begins as a **grassroots** effort in which **systems administrators** attempt to improve security of their systems.
- ***Key advantage;*** individual administrators possess in-depth knowledge and technical expertise that can greatly enhance the development of an information security system. These administrators know the **threats** to their systems and the **mechanisms** needed to protect them successfully.
- ***Key dis-advantage;*** seldom works because it lacks critical features such as **participant support** and organizational **staying power**.

Top-down Approach

- In top-down approach, the project is initiated by **upper-level managers** who issue policies, procedures and processes.
- Managers dictate the goals and expected outcomes; and also determine accountability for each required action.
- ***Key advantage;*** it has strong upper-management support, funding, a clear planning and implementation process, and the means of influencing organizational culture.
- The top-down approach has a **higher probability of success**.

Thank You!