Chapter one

Introduction to Information System Security

Objectives

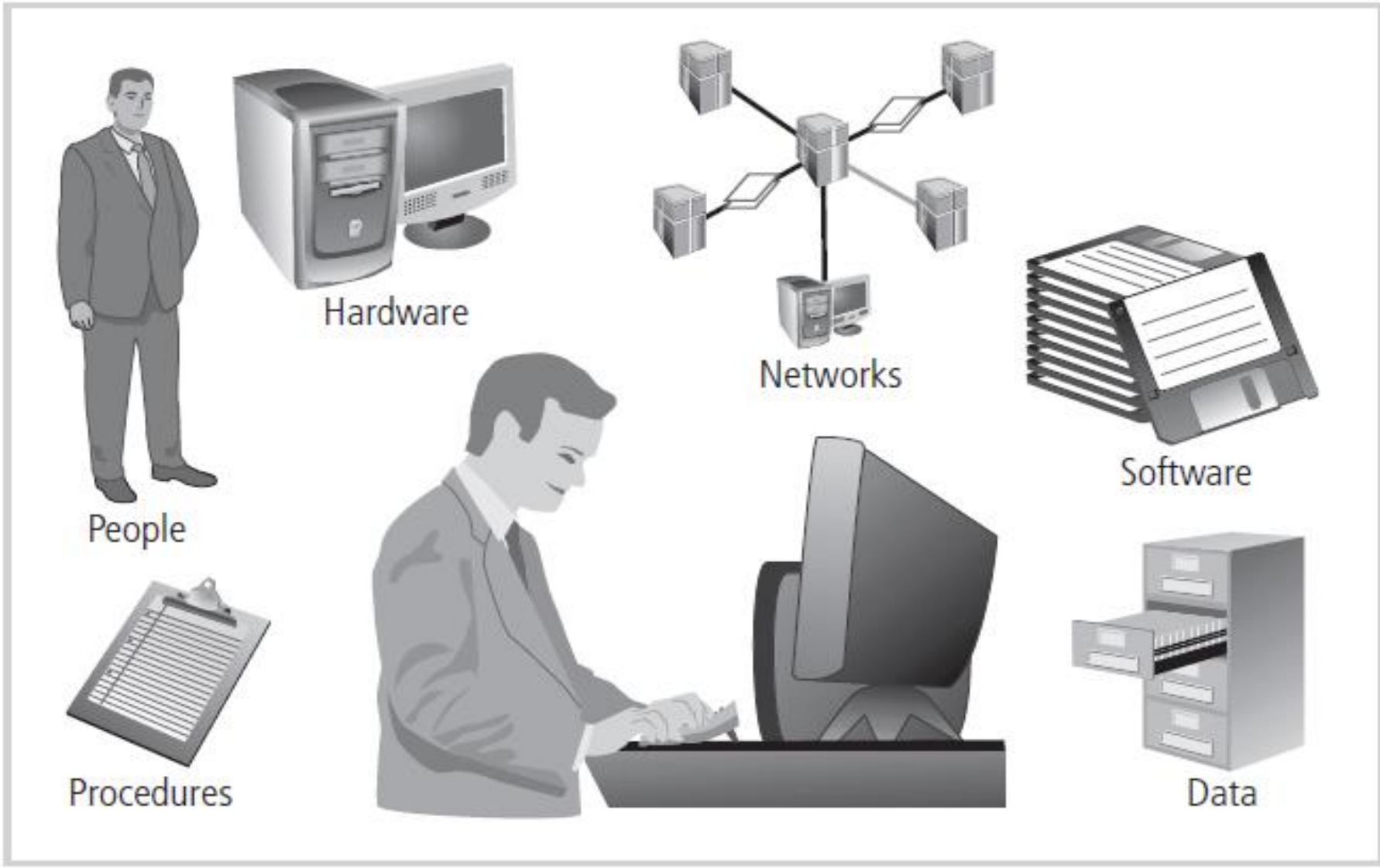
Upon completion of this chapter, you should be able to:

- 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 Information Systems?

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

Components of Information System



Traditional vs. Secured IS Components

Traditional System Components	SesSDLC Components	Risk Management System Components
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

Critical Characteristics of Information

The value of information comes from the characteristics it possesses:

- Confidentiality
- Integrity
- Availability
- Accuracy
- Authenticity

What is Security?

- "The quality or state of being secured—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 that uses, processes, stores, and transmits information
- The history of information security begins with **computer security**.
  - i.e Secure physical locations, hardware, and software from threats
- **Computer Security→Information Security→Cyber Security …. How are they different?? What are the historical developments??**
- **Necessary tools**: policy, awareness, training, education, technology

The need for Security

- **Organizations expend hundreds of thousands of dollars and thousands of man-hours to maintain their information systems. (Could be millions of Dollars)**
- **If threats to information and systems didn't exist, these resources could be used to improve the systems that support the information.**
- **However, attacks on information systems are a daily occurrence, and the need for information security grows along with the sophistication of such attacks.**

Business Needs First

Information security performs to provide four important functions for an organization:

1. **Protecting the organization's ability to function (Existence)**
2. **Enabling the safe operation of applications running on the organization's IT systems (An enabler)**
3. **Protecting the data the organization collects and uses (Privacy)**
4. **Safeguarding the organization's technology assets (Protection)**

Need to Know yourself and the enemy

- ***"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."***

~over 2,400 years ago by a Chinese General

- ***This Saying has importance in todays Information Systems Security.***
- ***In order to ensure security of systems, One has to know own strength and weakness and also the enemy's capability.***

Knowing Cont'd….

- **Know Your Self**
  - **First, you must identify, examine, and understand the information and systems currently in place within your organization.**
  - **This is self-evident.**
    - **To protect *assets*, which in computing are defined as *information* and *the systems that use, store, and transmit information*,**
    - **you must know what they are,**
    - **how they add value to the organization, and**
    - **to which vulnerabilities they are more susceptible**

Knowing yourself

- **Need to put appropriate security controls in place.**
- **Periodic review of controls is important**
  - **The policies**
  - **Education and training**
  - **Technologies that protect information must be carefully maintained and administered to ensure that they still remain effective**

Knowing the enemy

- **Having identified your organization's assets and weaknesses, it is important to**
  - **Identify, examine, and understand the *threats* facing the organization.**
  - **Determine which threat aspects *most directly affect the security of the organization* and its information assets, and then**
  - **Use the information to create a list of threats, each one ranked according to the importance of the information assets that it threatens. (Prioritizing risks of threats)**

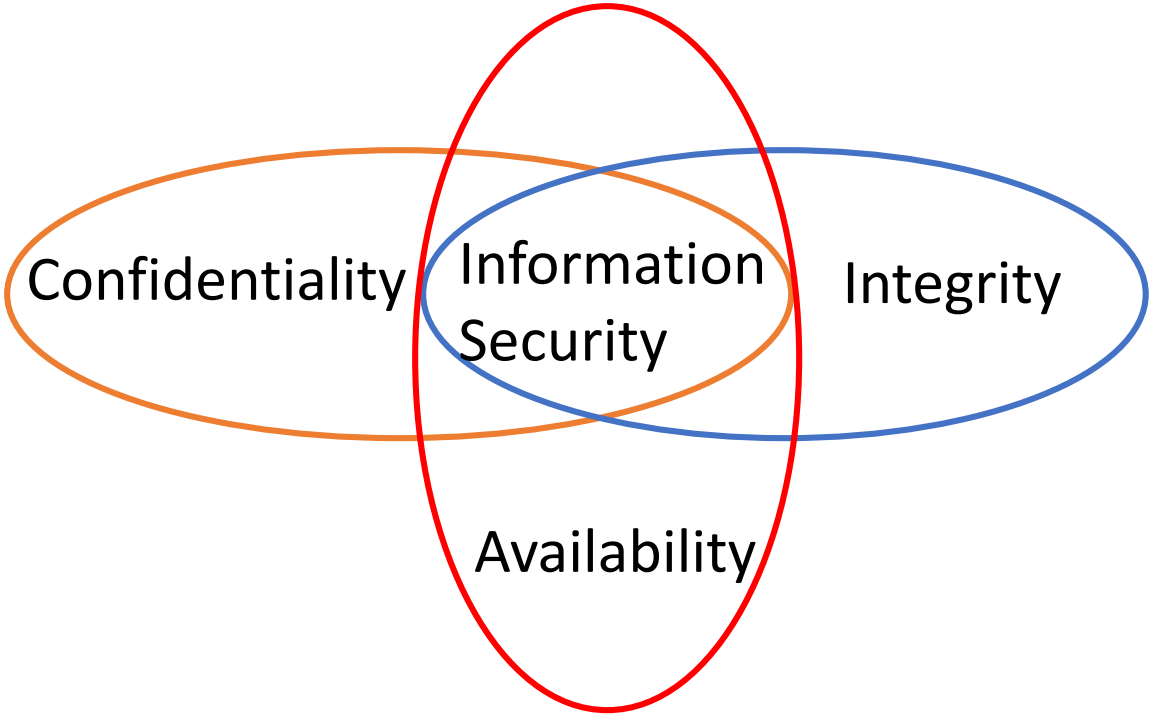
Approaches to IS Security Implementation

- The **bottom-up approach:** Information security can begin as a **grassroots effort in which systems administrators attempt to improve the security of their systems**. (at applications level)
- The **top-down approach:** In this case, the project is **initiated by upper-level managers** who issue policy, procedures and processes, dictate the goals and expected outcomes, and determine accountability for each required action - has a higher probability of success.

Securing Components in IS

- **Computer (software and hardware) is the key component in an information system**
- **Computer can be subject of an attack and/or the object of an attack**
  - **When used as the subject of an attack, computer is used as an active tool to conduct attack**
  - **When it is the object of an attack, computer is the entity being attacked**
  - **The attacks can also be of two types**
    - **Direct (the attack is directed to the computer itself and resources on it)**
    - **Indirect (the computer is attacked to cause problem to other system- e.g. DOS /DDOS**

Information Security: Basic Requirements also known as the security triads:(CIA)



Information Security: Basic Requirements

- ***Confidentiality*- it refers to information protection from unauthorized read operations(discloser)**
  - **the term *privacy* is often used when data to be protected belongs to individuals**
- ***Integrity* - it refers to information protection from modifications; it involves several goals**
  - **assuring that information and programs are changed only in a specified and authorized manner**

Information Security: Basic Requirements

- The integrity of information should be protected.
  - prevent loss, interception, misuse
  - maintain accurate, complete, timely data
  - no unauthorized alteration or destruction
- ***Availability*- it ensures that access to information is not denied to authorized (legitimate) subjects/users**

Key Information Security Concepts

- **Access:** A subject or object's ability to use, manipulate, modify, or affect another subject or object.
- **Asset:** The organizational resource that is being protected.
- **Attack:** 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.
- **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

Key Info. Security Concepts Cont'd…

- **Exploit:** is the act of trying to turn a vulnerability into an actual way to breach a system.
- **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.
- **Risk:** The probability that something unwanted will happen.
- **Subjects** and **objects:** A computer can be either the **subject of an attack—an agent entity** used to conduct the attack—or the **object** of an attack—**the target entity**

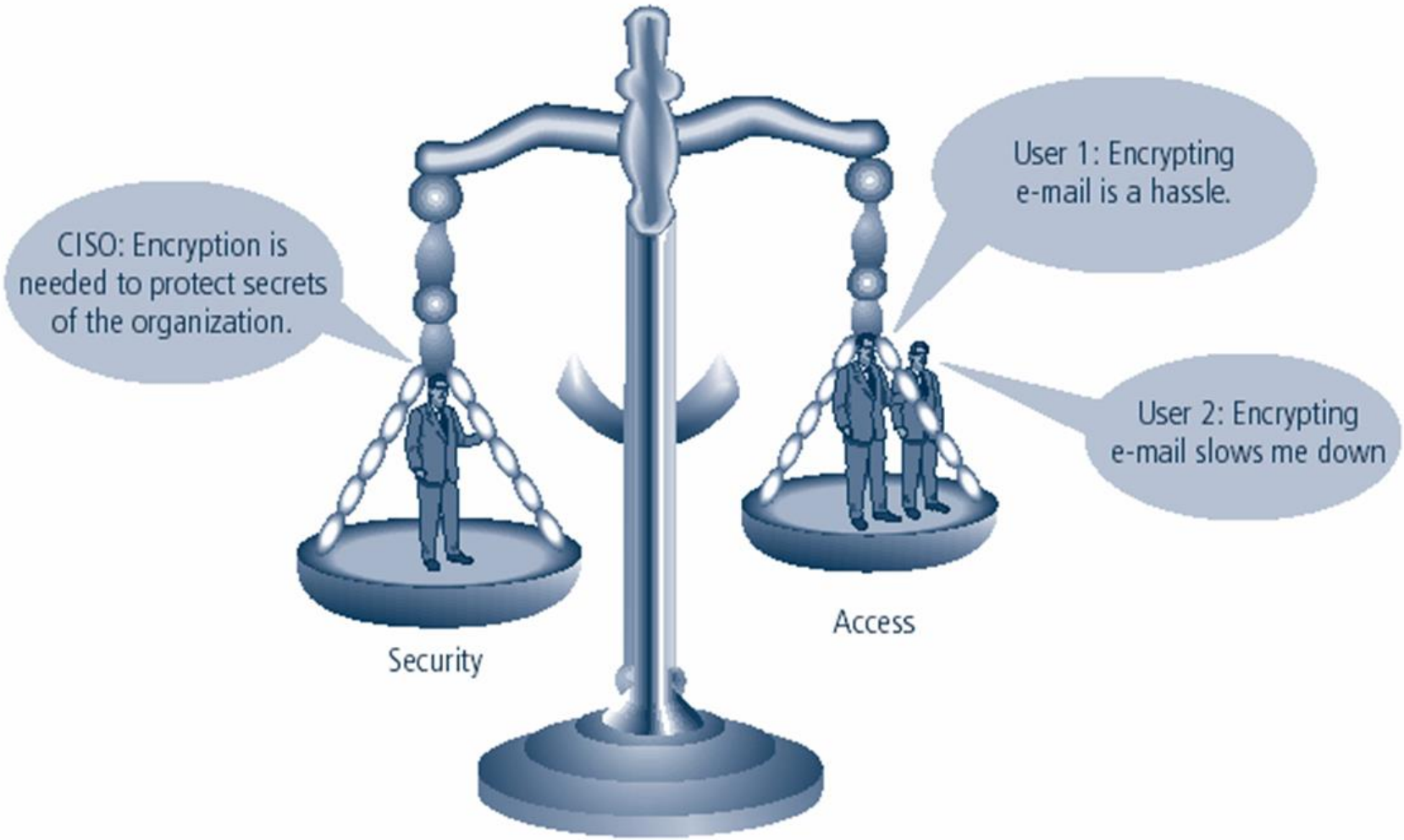
Key Info. Security Concepts Cont'd…

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

Balancing Information Security and Access

- Impossible to obtain perfect security—it is a process, not an absolute result/solution
- Security should be considered a balance between protection and availability (Access Vs Security).
- To achieve a balance, ***level of security must allow reasonable access, and yet protect against threats***

The balance


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

Definition of Privacy

- PRIVACY: The right of individuals to hold information about themselves in secret (private) , free from the knowledge of others
- **Privacy** is the ability of a person/organization to control the availability of private information.
- It is the “state of being free from unsanctioned intrusion”.

Privacy Cont'd…

- **Types of privacy** giving a rise to special concerns:
  - Political privacy
  - Consumer privacy
  - Medical privacy
  - *Information technology end-user privacy; also called data privacy (eg. Google's- gmail)*

CONFIDENTIALITY:

- **Confidentiality** refers to the duty of anyone entrusted with information to keep that information private.

Security

- SECURITY: The mechanisms by which confidentiality policies are implemented in computer systems, including provisions for:
  - Access control
  - Integrity
  - Availability
- *So, which one is the broader term? Privacy or Security?? Please find out…*

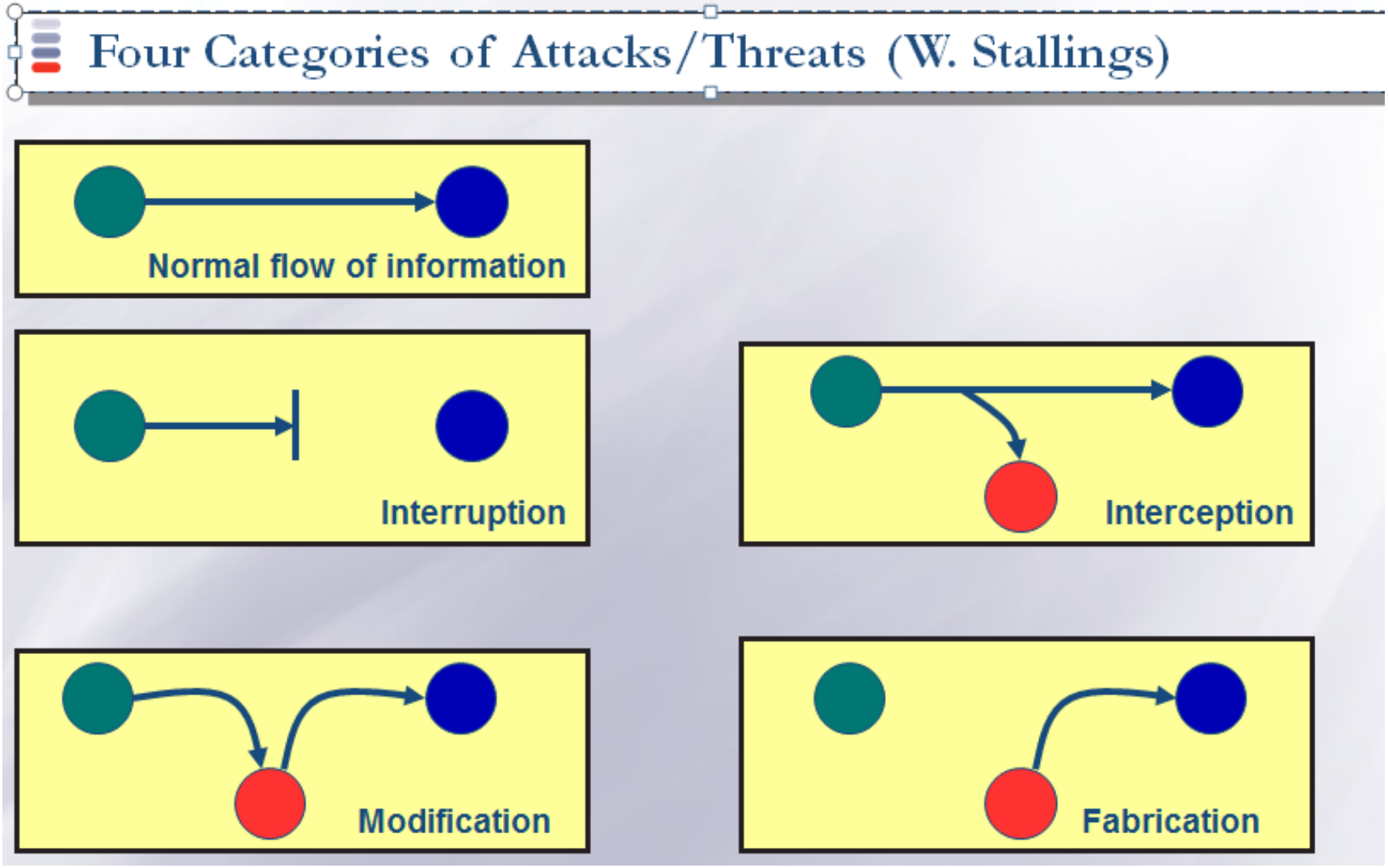
Information Security: how ?

- **Policies** define security and mechanisms to enforce the security goals, i.e.
  - Confidentiality
  - Integrity
  - Availability
- **Policy**: a statement of what is allowed and what is not allowed.
- **Mechanism:** a procedure, tool, or method of enforcing a policy.
  - **Security mechanisms** implement functions that help *prevent, detect, and respond to & recover* from security attacks.
  - *Cryptography* underlies many of the security mechanisms.

Category of Threats to Data/Information

- Disclosure
  - Release of potentially confidential data
- Deception
  - Acceptance of false data
- Disruption
  - Denial of service
- Usurpation
  - Unauthorized assumption of Control
- Modification
- Destruction

Categories of Network relate attacks



Goals of Security

- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers' violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

IS Security Life cycle

- It consists of:
  - first defining a *security policy*
  - then choosing some *mechanism* to enforce the policy
  - finally providing *assurance* that both the mechanism and the policy are sound

History of computer and Information Security

- **Until 1960s computer security was limited to physical protection of computers**
- **In the 1960s**
  - **Evolutions**
    - Computers became interactive
    - Multiuser/Multiprogramming was invented
    - More and more data started to be stored in computer databases
  - **Organizations and individuals started to worry about**
    - What the other persons using computers are doing to their data
    - What is happening to their private data stored in large databases

History Cont'd…

- **In the 1980s and 1990s**
  - **Evolutions**
    - Personal computers were popularized
    - LANs and Internet invaded the world
    - Applications such as E-commerce, E-government and E-health started to develop
    - Viruses become major threats
  - **Organizations/individuals started to worry about**
    - Who has access to their computers and data
    - Whether they can trust a mail, a website, etc.
    - Whether their privacy is protected in the connected world
- **and These Days?**
  - **Evolutions?**
  - **What makes people feel insecure the most?**

History Cont'd…

- **Famous security problems (*are these still famous or something new and extraordinary has happened??)***
  - **Morris worm – Internet Worm**
    - November 2, 1988 a worm attacked more than 60,000 computers around the USA
    - The worm attacks computers, and when it has installed itself, it multiplies itself, freezing the computer (Computers stuck)
    - It exploited UNIX security holes in Sendmail and Finger Programs (vulnerability points)
    - A nationwide effort enabled to solve the problem within 12 hours
  - Robert Morris (the father of Computer viruses) became **the first person (to create the first Internet worm "morris")** to be charged for the **Computer Fraud** and Abuse Act of 1986
    - He was sentenced to three years of probation, 400 hours of community service and a fine of some $10,000
  - He is currently a **Professor** at the Massachusetts Institute of Technology(MIT)
  - The First Virus--- "Creeper" (1971) – read more about this.

History Cont'd…

Famous security problems …

- **NASA** shutdown
  - In 1990, an Australian computer science student was charged for shutting down NASA's computer system for 24 hours
- **Airline** computers
  - In 1998, a major travel agency discovered that someone penetrated its ticketing system and has printed airline tickets illegally
- **Bank** theft
  - In 1984, a bank manager was able to steal **$25 million** through un-audited computer transactions

History Cont'd…

Famous security problems …

- In **Ethiopia**
  - Employees of a **company** managed to **change their salaries** by fraudulently modifying the company's database
  - In 1990s Internet password theft
    - *Hundreds of dial-up passwords were stolen and sold to other users*
    - *Many of the owners lost tens of thousands of Birr each*
  - A major company suspended the use of a **remote login** software by technicians who were **looking at** the computer of the General Manager
- In **Africa: Cote d'Ivoire**
  - An employee who has been fired by his company deleted all the data in his company's computer

Recent Security breaches…..

- User Account Credentials of world wide UN officials were hacked by a hacking group(though UN denounces the accounts are no longer active)
- The Sony PlayStation Network outage:
  - The outage occurred in 2011 on Sony's PlayStation Network in which personal details from approximately 77 million accounts were stolen and prevented users of "PlayStation 3" and "PlayStation Portable consoles" from playing online through the service. The outage lasted for approximately 23 days
- Stuxnet Hits Iran
  - News broke out(in 2011) that five Iranians suspected in enriching weapons-grade uranium were hit by the Stuxnet worm over a 10-month period or even more(since 2007), one reported incident caused damage to a main centrifuge. A similar (to stuxnet) virus named Flame was discovered by kaspersky lab lately.
- The Twitter Account Hacking in 2013-
  - nearly 250,000 personal Accounts were hacked.

Recent Security Breaches cont'd…

- In what was probably the largest theft of data ever, from off-price department stores T.J. Maxx and Marshalls. The hacker, Albert Gonzalez, was only caught in 2008; in 2010, he was sentenced to 20 years in federal prison.
  - Between 2005 and his arrest in 2008, Gonzales stole the details of over 170 million credit and debit card numbers, making him the most successful credit card thief of all time.
- In November 2007, the United Kingdom's Revenue & Customs service lost computer discs that contained the names, addresses, and National Insurance numbers of 25 million British citizens. Similar incident happened to US Social Security Service records.
- RSA Security — March 2011
  The worst (and undoubtedly ***the most ironic***) data breaches happen when ***security companies themselves get hacked***. Kaspersky and Symantec, developers of antivirus and security software, have been hacked multiple times — and in March 2011, one of the biggest players, RSA Security, had a sensitive and highly confidential internal database laid bare. The theft of RSA's database mapping token serial numbers to the secret token "seeds"- RSA's SecureID two factor Authentication method.

The Gawker Media Hack

- **Who:** Gnosis
- **When:** December 2010
- **What happened:** The email addresses and passwords for more than 1.3 million readers of Gawker Media's websites—including Gawker, Gizmodo and Lifehacker—were compromised in this breach. A hacker group calling itself Gnosis claimed responsibility for the incident, which resulted in millions of accounts on ***other*** networks being hijacked due to people using the same password for multiple sites (sound familiar?).
- Along with stealing the user data, the group also managed to snag the source code for Gawker's proprietary content management system, leading to a major (and likely expensive) overhaul in the period following the attack.

The KT Corporation Hack

- **Who:** Unknown hackers
- **When:** February–July 2012
- **What happened:** One of the most wired countries in the world fell prey to a massive theft of digital data that year when two men allegedly stole user information from more than 8 million KT mobile phone subscribers in South Korea. The hackers sold the data to various marketing companies, which reportedly used the information to solicit subscribers and convince them to switch to another service providers
- Want more??? See the following.
  - *Connecting the dots: A timeline of technologies, threats and regulations that redefined cybersecurity and privacy*

https://www.pwc.com/us/en/cfodirect/issues/cyber-security/information-security-survey.html

Security /Privacy :legal Issues

Early Efforts

- 1960s: Marked as the beginning of true computer security system development
- 1970s: Tiger teams
  - Government and industry sponsored hackers who attempted to break down defenses of computer systems in order to uncover vulnerabilities so that patches can be developed
- 1970s: Research and modeling
  - Identifying security requirements
  - Formulating security policy models
  - Defining recommended guidelines and controls
  - Development of secure systems

Legal Issues- *National* .. Cont'd…

- In the US, legislation was enacted with regards to computer security and privacy starting from late 1960s. In 2002, the Federal Information Security Management Act (FISMA) - United States federal law enacted.
- European Council (EU) adopted a convention on Cyber-crime in 2001.
- Under a recent security policy proposals, each EU country would have to appoint a Computer Emergency Response Team (CERT) and create an authority to whom companies would report breaches. (Who in Ethiopia?)
- The World Summit for Information Society considered computer security and privacy as a subject of discussion in 2003 and 2005.
- In 2013, the World Information Security Summit featuring topic as Mobile Networking and Security. (The Cloud and the Tablets becoming the next generation of computing)
- The Ethiopian Penal Code of 2005 has articles on data and computer related crimes (what does it say? -- read!)

Legal issues- *Global* –the Challenges

- **Different Countries have different stands regarding Cyber crime and its legal consequences.**
- **Recently , efforts have been seen to have a global Convention / or Policy on cyber crime and legal accountabilities.**
- **The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or just the Budapest Convention (was enacted in 2004), is the first international treaty seeking to address Computer crime and Internet crimes by harmonizing national laws.**
  - **US has been the main player on this Convention and is pushing the UN to make it a Global Convention.**
  - **Focuses on Specific issues of Cyber Crime.**
  - ***The 32nd Article "cross-border access"* which allows intelligence agencies of some countries to penetrate the computer networks of other countries and to conduct operations there without the knowledge of the national authorities, *caused disagreement between nations*.**
  - **Hence, that is not Globalized so far.**

Global Information Security Policy –Challenge cont'd…

- **The UN , " International Convention on Information security – a concept " was drafted with Russia's leading role in July 2012.**
  - The convention has 23 Articles on Global Information Security policies.
  - Focuses on all wrongful (hostile) use of information or Information and Communication Technologies (ICTs)
  - This version of the Convention has support of many countries from Europe, Africa, Asia and Latin America.
  - It is more probable that this version of the convention will be the UN convention.
  - But Some Countries including US don't agree on the details and are still fighting over it.
  - Hence No Global Solution.(Is there any solution now?!)

Security/Privacy - Vulnerabilities

- **Physical vulnerabilities (Eg. Buildings design)**
- **Natural Vulnerabilities (Eg. Earthquake)**
- **Hardware and Software Vulnerabilities (Eg. Failures, overflows)**
- **Media Vulnerabilities (Eg. Disks can be stolen)**
- **Communication Vulnerabilities (Eg. Repudiation, Wires can be tapped)**
- **Human Vulnerabilities (Eg. Insiders, Outsiders) the Greatest of all vulnerabilities**
  - **Exploiting Vulnerabilities has its own cost. An attacker will not try to exploit if the cost is more than what s/he is trying to get.**