8/8/2022

UNIT - I

INFORMATION SYSTEM

by

Mr. Ajay Kumar Badhan

Assistant Professor

M.TECH[CST], B.TECH [CSE]

Email: ajay.27337@lpu.co.in

Personal Blog: https://ajaykumarbadhan.wordpress.com/

Preferred Text Book

- Information System Security Wiley Publications by Nina Godole, Wiley
- Computer Security: The Complete Reference Roberta: Tata Mcgraw Gill by Bragg, Mcgraw Hill Edition

CONTENT

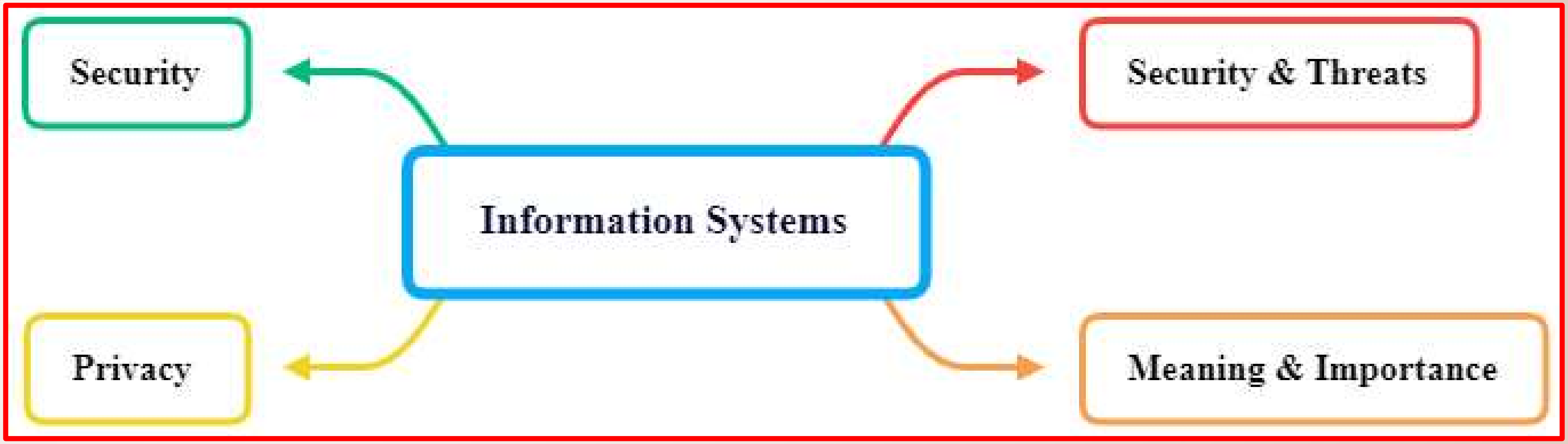
INFORMATION SECURITY

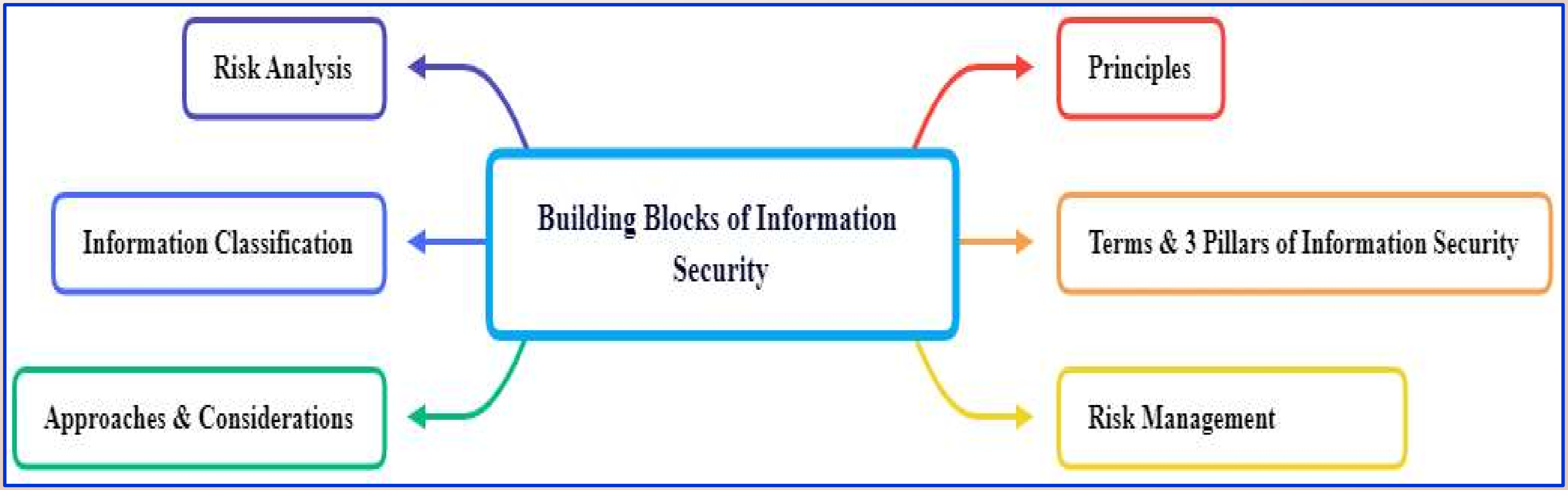
- Information Security & Threats
- Meaning of Information System
- Importance of information System
- Information Security
- Privacy Threat

BUILDING BLOCKS

- Principles
- Terms
- Three Pillar of Information Security
- Risk Management
- Risk Analysis
- Information Classification
- Approaches and Considerations

CONTENT - GRAPHICAL PRESENTATION

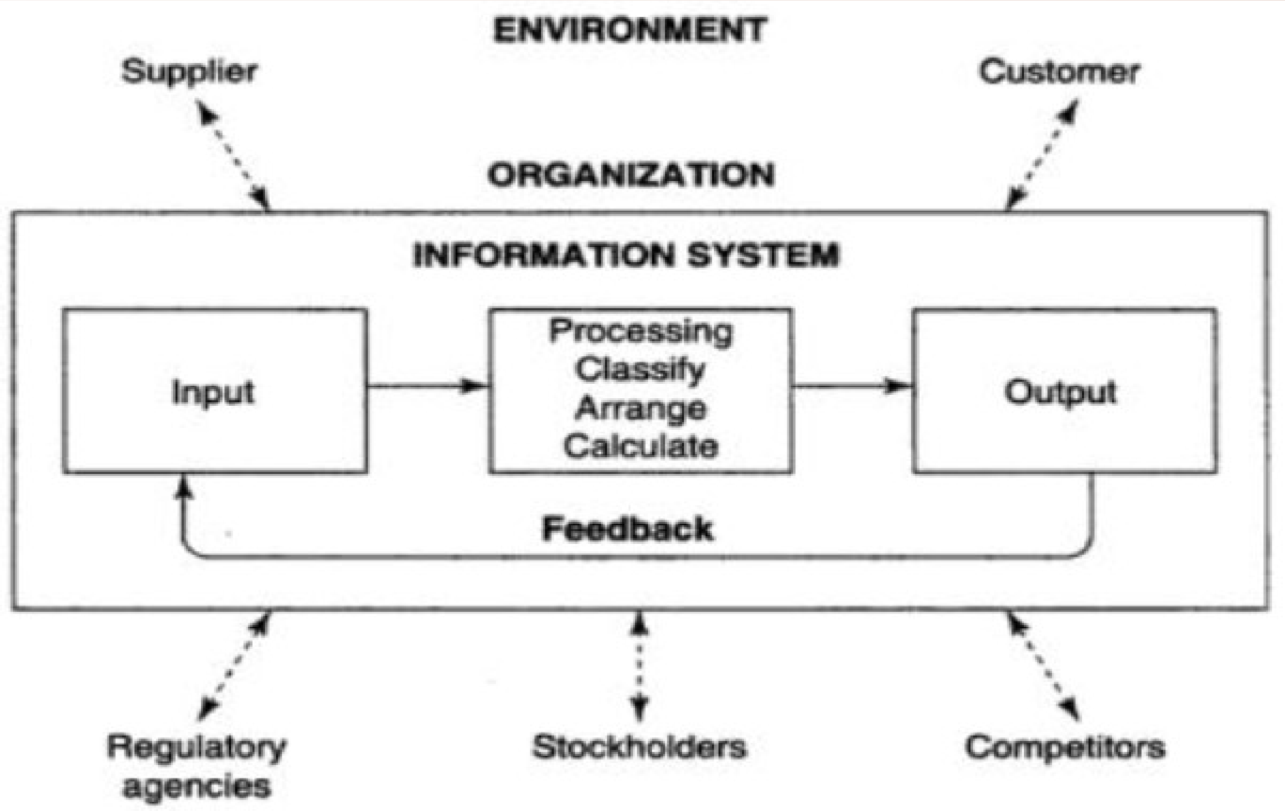



Building Blocks of Information Security
Risk Analysis
Principles
Information Classification
Terms & 3 Pillars of Information Security
Approaches & Considerations
Risk Management

INTRODUCTION – INFORMATION SYSTEM

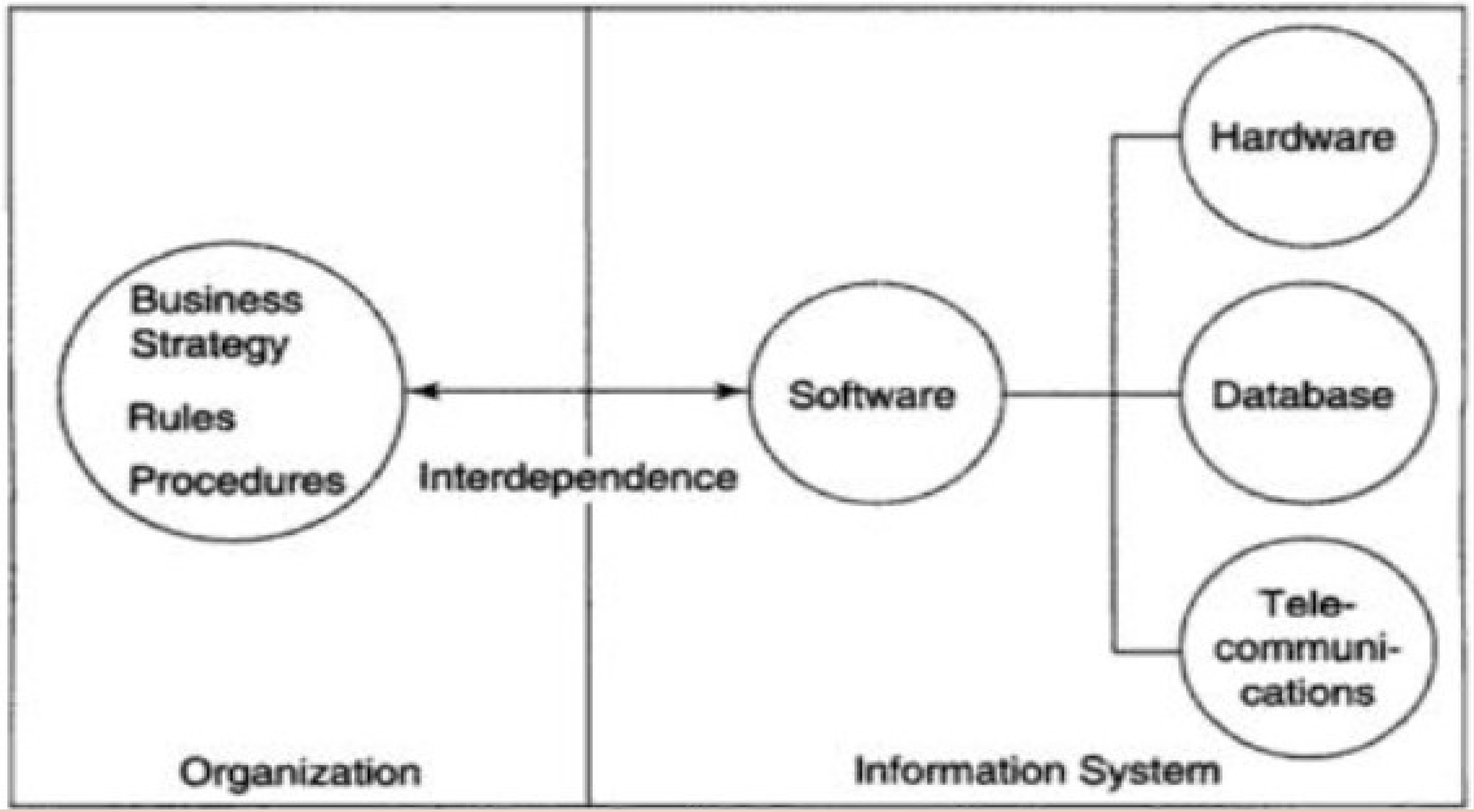
Basic Introduction

1. An Information system is a group of components that interact to produce information
2. It is an **integrated** and **cooperating** set of **software-directed information technologies** supporting individual, group, organizational, or societal goals.
3. It is the study of complementary networks that people and organizations use to collect, filter, process, create, and distribute data.



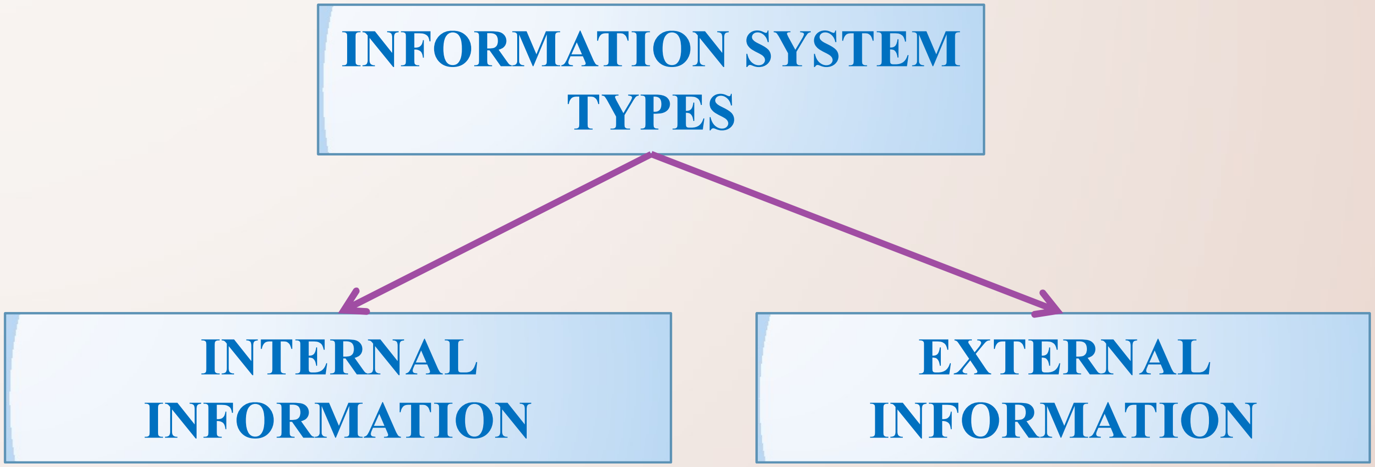
INTRODUCTION – INFORMATION SYSTEM

Functions of Information System



INFORMATION SYSTEM - TYPES

Information System



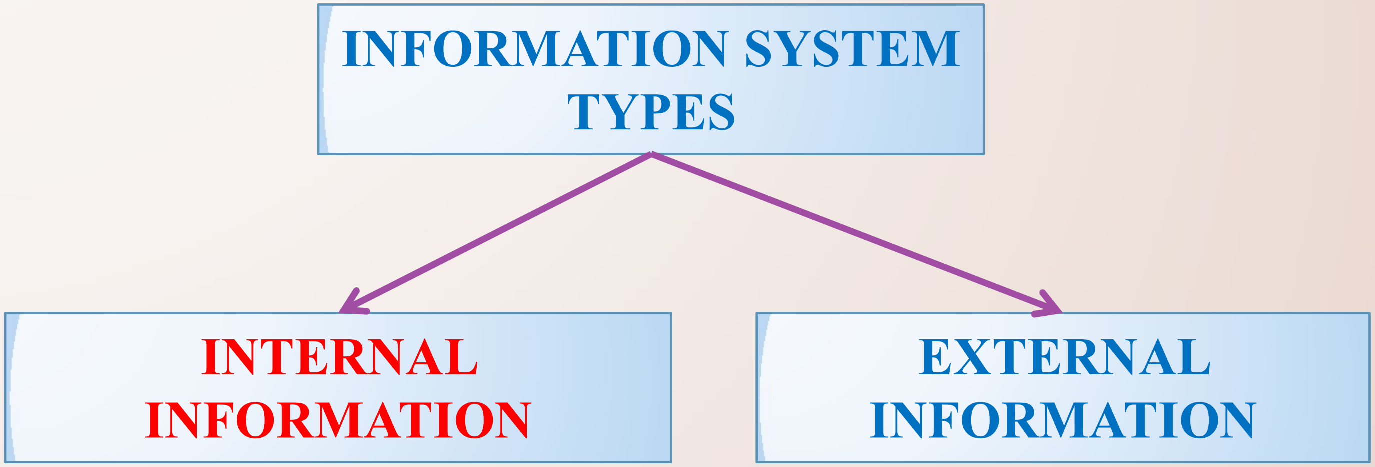
INFORMATION SYSTEM TYPES

INTERNAL INFORMATION

EXTERNAL INFORMATION

INFORMATION SYSTEM - TYPES

Information System



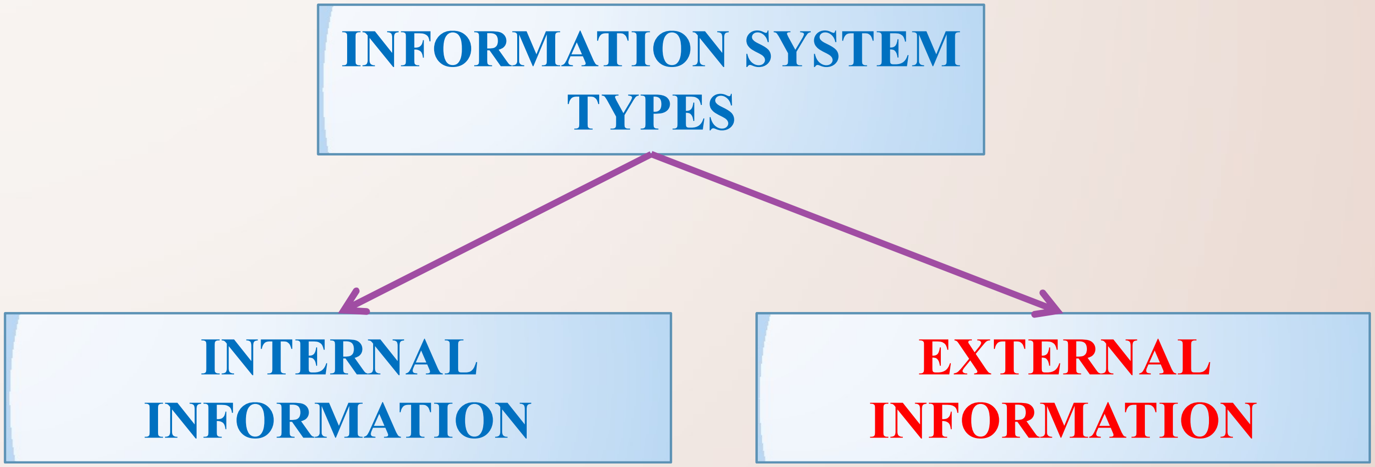
INTERNAL INFORMATION

1. The information which is collected from the **sources**, **internal to the organization** is called Internal Information.
2. This information is generated from the operations of the organization at the various **functional levels**
3. They always pertain to the various operational units of the organization.
4. The internal information is generally required by the **middle** or **supervisory level of management**

Examples: Production figures, **sales forecast**, **budgets**, **stock level**, **employee data**, **accounting reports**

INFORMATION SYSTEM - TYPES

Information System



INFORMATION SYSTEM TYPES

INTERNAL INFORMATION

EXTERNAL INFORMATION

EXTERNAL INFORMATION

1. The information which is collected from the sources **external to the organization** is called External Information.
2. These are generated in the **external environment** of the organization
3. They are considered to **affect** the organizational performance in the external environment
4. It is generally required by **top-level management**.
5. It is used in the **planning process of management** to give the shape of its future.

Examples: Govt. Policies, **Economic Trends**, **Market Information**, **Competitive Information** etc

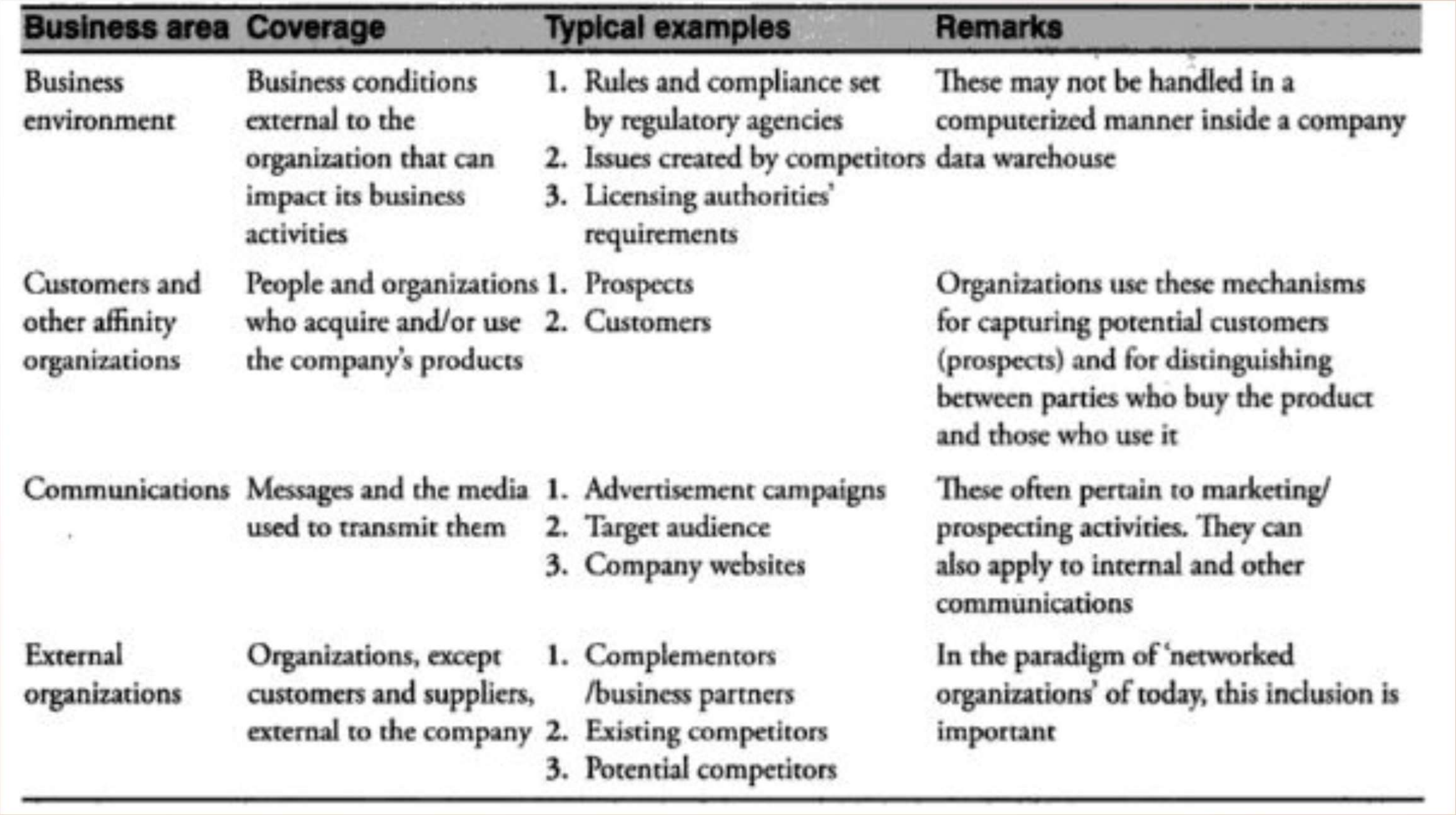
INFORMATION SYSTEM - INTRODUCTION

Information System Roles & It's Management

1. It helps managers in effective **decision-making**
2. Based on IS, organization will gain edge in the competitive environment.
3. IS helps taking **right decision** at the right time.
4. Knowledge gathered through Information System is useful in unusual situation.
5. It can be integrated to formulate a strategy of action.
6. It ensures **pervasiveness** of decision making.
7. It makes the organization transparent
8. It helps managerial learning about organization.

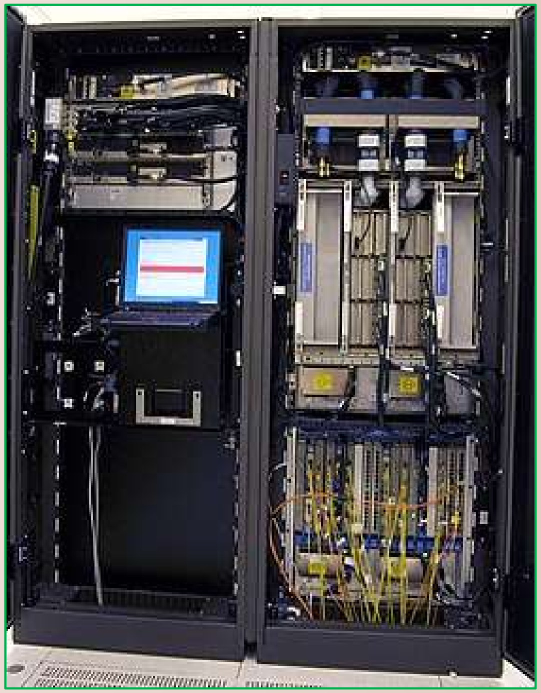
INFORMATION SYSTEM - INTRODUCTION

Business Area Wise Organization of Information



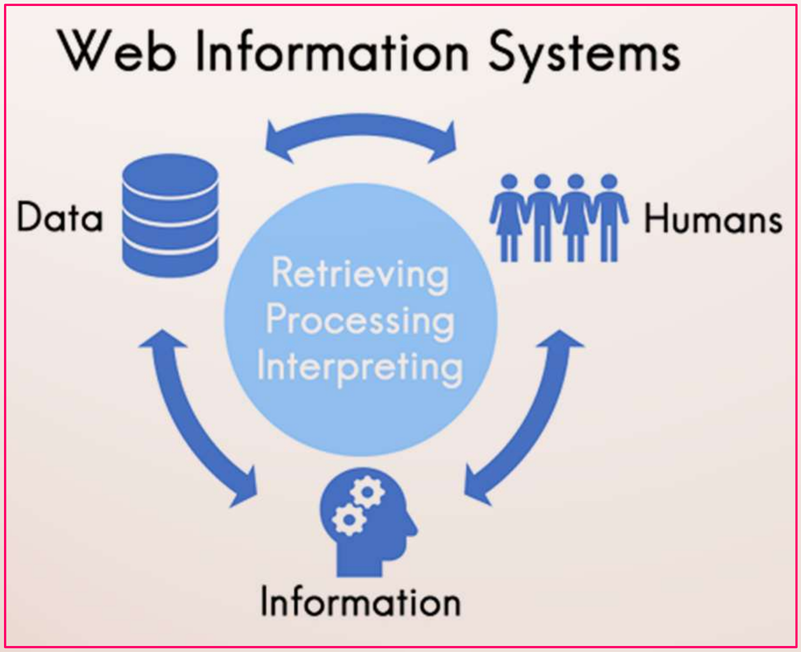
Business area	Coverage	Typical examples	Remarks
Business environment	Business conditions external to the organization that can impact its business activities	1. Rules and compliance set by regulatory agencies 2. Issues created by competitors 3. Licensing authorities' requirements	These may not be handled in a computerized manner inside a company data warehouse
Customers and other affinity organizations	People and organizations who acquire and/or use the company's products	1. Prospects 2. Customers	Organizations use these mechanisms for capturing potential customers (prospects) and for distinguishing between parties who buy the product and those who use it
Communications	Messages and the media used to transmit them	1. Advertisement campaigns 2. Target audience 3. Company websites	These often pertain to marketing/ prospecting activities. They can also apply to internal and other communications
External organizations	Organizations, except customers and suppliers, external to the company	1. Complementors /business partners 2. Existing competitors 3. Potential competitors	In the paradigm of 'networked organizations' of today, this inclusion is important

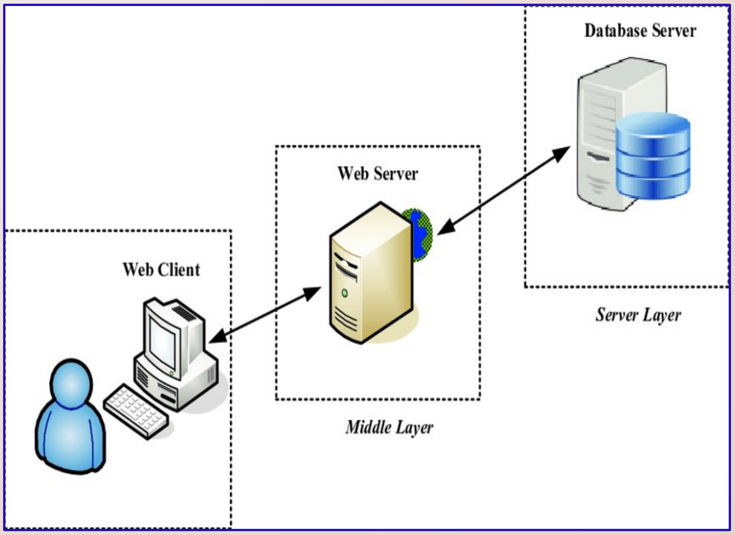
INFORMATION SYSTEM - INTRODUCTION



Changing Nature of Information System

1. Maine Frame Based Information System
2. Client-Server based Information System
3. Web-based Information System





INFORMATION SYSTEM – Security & Threat

Mis-use of Information systems leads to:

1. **Loss of Productivity**
2. **Loss of Revenue**
3. **Legal Liabilities**
4. **Work Place issues**

PILLARS OF INFORMATION SECURITY

The CIA triad refers to an information security model made up of the three main components:

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

CONFIDENTIALITY

1. It is used to prevent the **intentional** or **unintentional** unauthorized disclosure of message content
2. It can occur in many ways, such as through the intentional release of **private information of a company** or **through a misapplication of network rights**.
3. Confidentiality is concerned with **preventing** the unauthorized disclosure of sensitive information
4. It is associated with **secrecy** and the use of **encryption.** It means the data is only available for authorized parties.

Example: Bank never gives information about a client to another person.

Some more examples:

1. Suppose there a computer in which there is some important data is saved. Confidentiality means there should be a trust that data will be accessed by you or a dedicated user only. Access to that data will be only through an authorized person.

PILLARS OF INFORMATION SECURITY

The Three Pillars of Information Security are:

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

INTEGRITY

1. It refers to the certainty that the data is **not tampered** with or degraded during or after submission.
2. It means no one can modify or later contents of information other than the owner.
3. Prevention of the modification of information by unauthorized users.

   Example: Suppose user-1 sends a message "**Hi**" to user-2. The message sent should not be modified in between
3. Preservation of the **internal** and **external** consistency
4. Internal consistency ensures that data is consistent.

Examples:

1. Only authorized users can change the password of their Facebook account. Internally data should be maintained
2. No one can do transactions from a user account except the user itself.

PILLARS OF INFORMATION SECURITY

The Three Pillars of Information Security are:

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

AVAILABILITY

1. It assures that a **system's authorized** users have timely and uninterrupted access to information in the system and to the network.
2. It means that the **information** is available to the authorized user when it is needed.
3. For a system to demonstrate availability, it must have properly **functioning computing systems**, **security controls**, and **communication channels**.
4. Systems defined as **critical** often have extreme requirements related to availability.

Example: The user wants to access the FB account during midnight, the server should be available to serve it

INFORMATION SECURITY - TERMS

Important Terms

1. **Identification** **2. Authentication** **3. Accountability** **4. Authorization**

IDENTIFICATION

1. It indicates the means by which users claim their identities to a system. It is most commonly used for **access control** and is necessary for **authentication** and **authorization**.
2. It is the ability to identify uniquely a user of the system or an application that is running in the system

Examples: Login ID, Identity Card of employees in any organization

AUTHENTICATION

1. It is the **testing** or **reconciliation** of evidence of the user's ID. It establishes a user's ID and ensures that the user is who they say they are.
2. It is the ability to prove that a user or application is genuinely who or what the application claims to be.
3. It is a **security measure** designed to establish the **validity of a transmission**, **message**, or **originator** or a means of verifying an individual's eligibility to receive specific categories of information

INFORMATION SECURITY - TERMS

Important Terms

1. **Identification** 2. **Authentication** 3. **Accountability** 4. **Authorization**

ACCOUNTABILITY

1. A system's ability to determine the actions and behavior of a single individual within a system and to identify that particular individual. Audit trails and los support accountability

Examples:

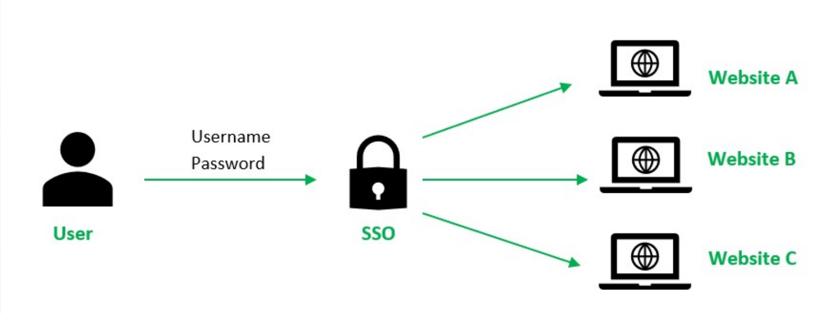
AUTHORIZATION

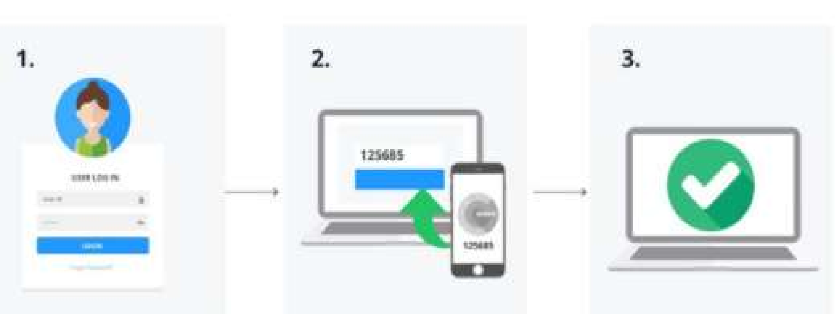
1. The rights and permissions granted to an individual (or process), which enables access to a computer resource.
2. Once the user identity and authentication are established, authorization levels determine the extent of system rights that an operator can hold. It is the access rights granted to the user, program, or process.
3. It protects critical resources in a system by limiting access to the resources to authorized users and their applications. It prevents the unauthorized use of resources.

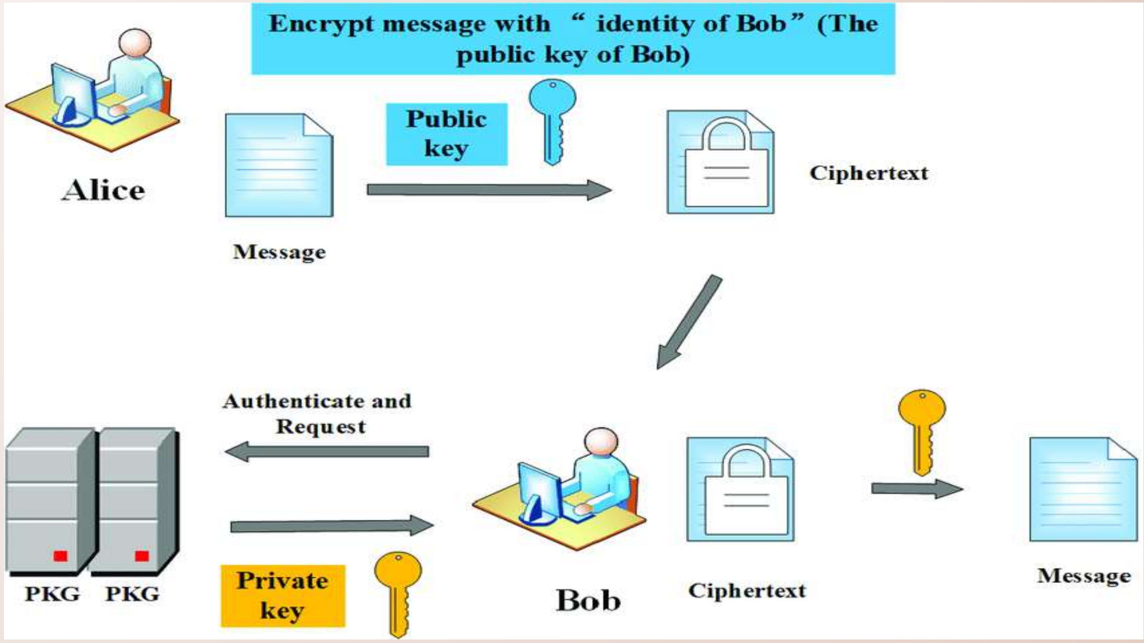
INFORMATION SECURITY - TERMS

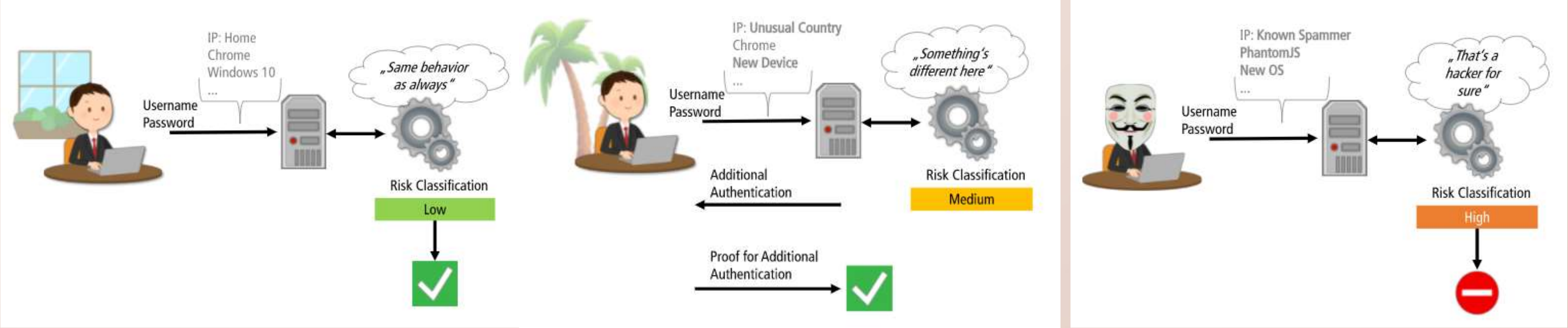
Important Terms

1. Identification
2. Authentication
3. Accountability
4. Authorization





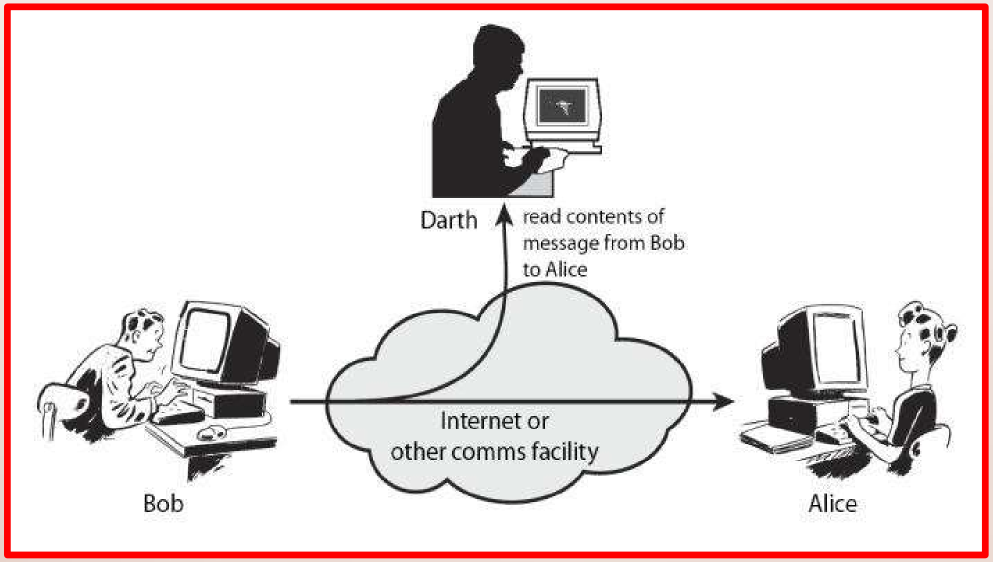


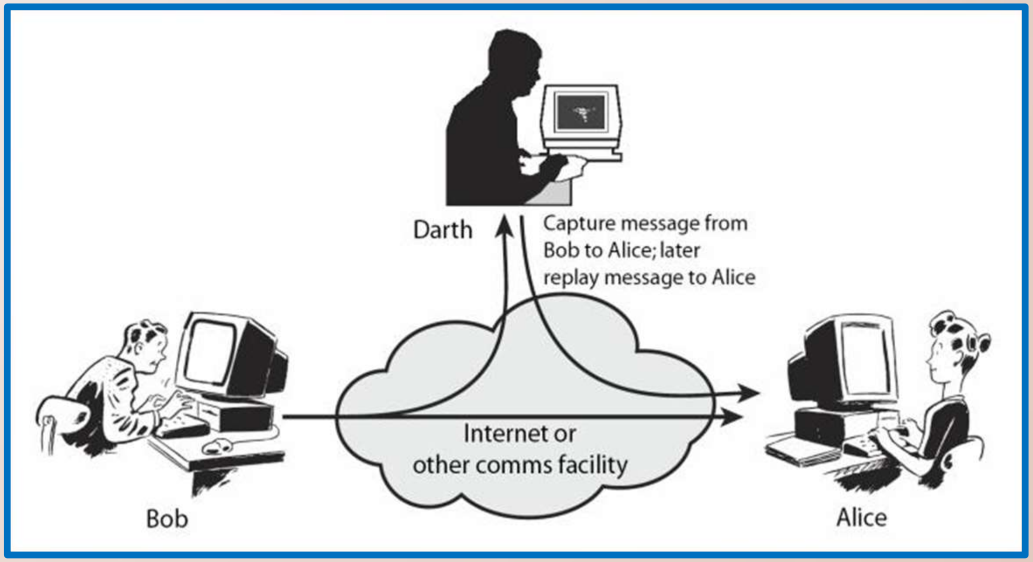


INFORMATION SECURITY - ATTACKS

Security Attacks

1. Any action that compromises the security of information owned by another organization
2. Information Security is about how to prevent attacks or falling, to detect attacks on information-based systems
3. Have a wide range of attacks:
   1. **Passive Attack** ⇒ In this the attacker observes the messages and copies them
   2. **Active Attack** ⇒ In this, the attacker tries to modify the content of the messages.


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


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

INFORMATION SECURITY - ATTACKS

Basic Terms in Security Attacks:

There are 3 terms:

1. **Threat** ⇒ It is an object, person, or other entity that represents a constant danger to an asset.

2. **Vulnerability** ⇒ A weakness that allows an attacker to reduce the systems information assurance.

   At the intersection of **3** elements:

   a. **system susceptibility of the flaw**,

   b. **attacker access to the flaw**,

   c. **attacker capability to exploit the flaw.**

3. **Countermeasures** ⇒ The measures that are implemented to overcome the threats and vulnerabilities.

   Examples: Cryptography, Ciphertext, Cesare Cipher etc.

INFORMATION SECURITY - ATTACKS

Information Level Threats

1. Spreading wrong information ex- hoaxes
2. Involves purposeful dissemination of information
3. Sending fake inquiries
4. Setting up revenge websites
5. Falsifies Job advertisements

Network-Based Threats

1. Hacking of Computer System
2. Denial of Service

DOS

1. Flooding accounts with a large number of emails is a network-based attack as it is the size and the quantity of the email that matters and not the content of the email.
2. Before the rise of the internet attacks were physical but nowadays attacks are through networks.

Example: Amazon Web Services (AWS) reports that in February 2020, they defended against a **2.3 - terabit-per-second (Tbps) distributed denial of service (DDoS) attack!**

INFORMATION SECURITY - PRINCIPLES

Principle Source of Security Threats

1. **Human Error:**

   When an employee discloses confidential information it comes under human error.

2. **Computer Abuse or Crime:**

   When a person intends to be malicious ex fake rumors like you have won a lottery

3. **Natural Disasters:**

   This can happen in the form of natural calamities, wars, and riots.

4. **Failure of Hardware and Software:**

   Server malfunctioning and software errors

INFORMATION SECURITY - PRINCIPLES

Security Threats Related to Computer Abuse or Crime

1. **Impersonation:**

   The impersonator enjoys the privileges of a legitimate user by gaining access to a system by identifying oneself as another person after having defeated the identification and authentication controls employed by the system.

2. **Trojan Horse**

   Concealing within an authorized program a set of instructions that will cause unauthorized actions.

3. **Logic Bombs:**

   unauthorized actions are often introduced with the Trojan horse technique, which stays dormant until a specific time comes, as the instruction may keep checking the system's internal clock.

4. **Computer Virus:**

   A segment of code that is able to perform malicious acts and insert copies of themselves into other programs in the system. Because of this replication, a virus will progressively infect healthy programs and systems.

INFORMATION SECURITY - PRINCIPLES

Security Threats Related to Computer Abuse or Crime

5. **Denial of Service (DOS):**

   Rendering the system unusable by legitimate users.

6. **Dial Diddling**

   Changing data before or during input, often to change the contents of a database.

7. **Salami Technique:**

   Diverting the small amount of money from a large number of accounts maintained by the system. These small amounts will not be noticed.

8. **Spoofing:**

   Configuring a system to masquerade as another system on the network in order to gain unauthorized success.

9. **Super-Zapping:**

   Using a system's program that can bypass regular system controls to perform unauthorized acts.

10. **Scavenging**

    Unauthorized access to information by searching through the residue after a job has been run on a computer. E.g. printer.