Parul® University
Vadodara, Gujarat

NAAC GRADE A++

Information Security

Shraddha Gaur
Department of IT
PIET, Parul University

What is Information System?

What is Information System?

- An information system (IS) is a set of interconnected components that collect, process, store, and distribute information to support decision-making, coordination, control, analysis, and visualization in an organization.

(Or)

- Information systems (IS) is the study of complementary networks of hardware and software that people and organizations use to collect, filter, process, create, and distribute data.

(Or)

- Information systems are combinations of hardware, software, and telecommunications networks that people build and use to collect, create, and distribute useful data, typically in organizational settings

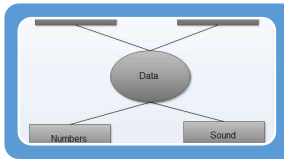
Components of Information System?

Hardware

• Physical devices like computers and servers.

Software

• Programs and applications for data processing.



Data

• Raw facts and figures

Procedures

• Methods and rules governing system operation.

People

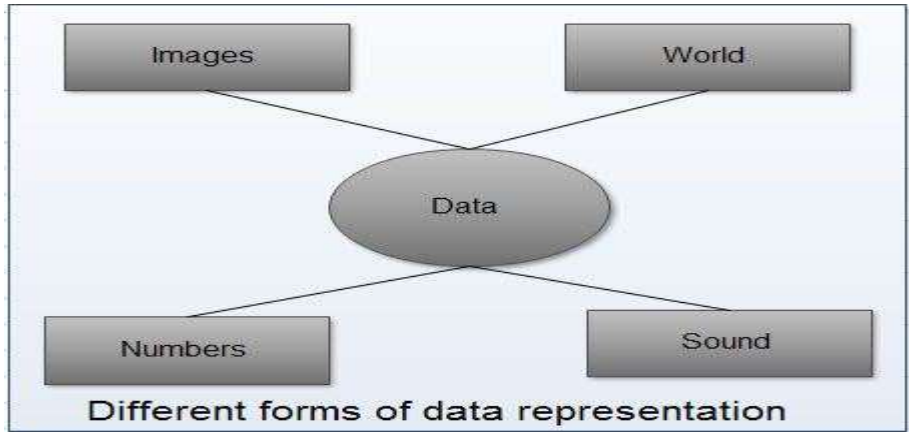
• Users, administrators, and stakeholders.

People?

- **People Resource:** People are considered part of the system because without them, systems would not operate correctly. In Information system there are two kinds of people resource -
- (i) **End User:** also called users or clients, are people who actually use the information system or its products. Eg. Customers, salesperson, engineers, clerks, managers
- (ii) **IS Specialist:** also called IS developers, are people who develop the information system and its components. Eg. System Analysts (who design IS based of requirements of end users), Software developers (create computer programs based on specifications of analysts), System Operator (who help monitor and operate large computer system and networks) and other Managerial, Technical, Clerical IS personnel.

Data?

- **Data Resource:** Data resources include data (which is raw material of information systems) and database. Data can take many forms, including traditional alphanumeric data, composed of numbers and alphabetical and other characters that describe business transactions and other events and entities. Text data, consisting of sentences and paragraphs used in written communications; image data, such as graphic shapes and figures; and audio data, the human voice and other sounds, are also important forms of data.



Different forms of data representation

Data?

- Data resources must meet the following criteria:
- **Comprehensiveness:** It means that all the data about the subject are present in the database.
- **Non-redundancy:** It means that each individual piece of data exists only once in the database.
- **Appropriate structure:** It means that the data are stored in such a way as to minimize the cost of expected processing and storage.
- The data resources of IS are typically organized into:
- Processed and organized data - Databases
- Knowledge in a variety of forms such as facts, rules, and case examples about successful business practices

Procedures?

- Procedures in the context of information systems refer to the step-by-step instructions or processes that individuals follow to accomplish a specific task or goal within the system.

- **Purpose:**

  Procedures serve to standardize and streamline processes within an organization or system.

  They ensure consistency in how tasks are carried out, reducing the likelihood of errors and improving efficiency.

Procedures?

Task-specific:

- Each procedure is designed for a specific task or set of related tasks.
- For example, there may be procedures for data entry, system maintenance, security protocols, etc.

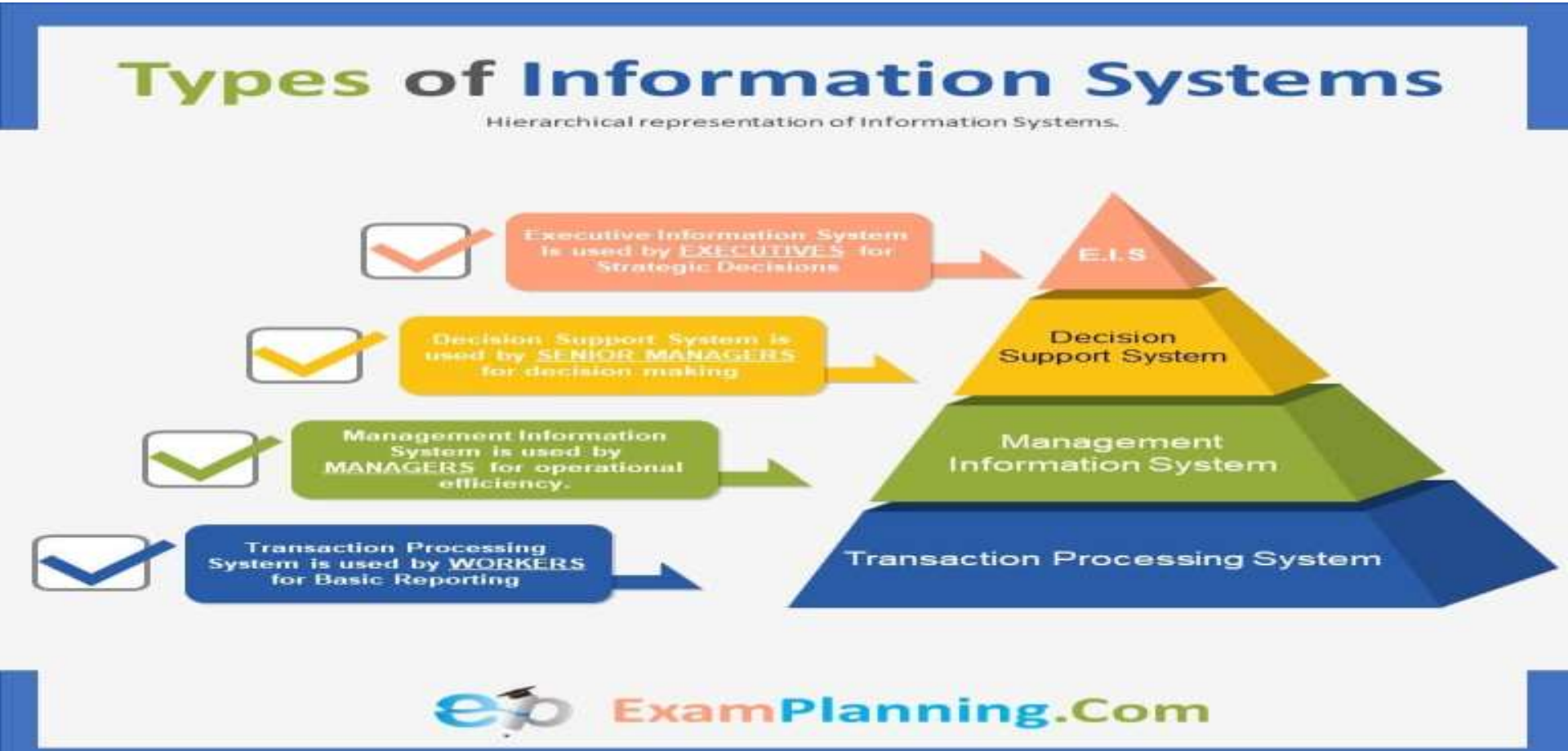
Monitoring and Evaluation:

- Procedures provide a basis for monitoring and evaluating the performance of tasks.
- By following documented procedures, organizations can assess efficiency, identify bottlenecks, and improve processes over time.

Audit and Accountability:

- Procedures contribute to the accountability of individuals and the organization as a whole.
- In the event of audits, procedures provide a basis for assessing compliance and identifying areas for improvement.

Types of Information Security



Types of Information Security

- Transaction processing system
- Decision support system
- Executive information system
- Management information system
- Enterprise resource planning and
- Expert systems.
- Online Analytical Processing (OLAP)

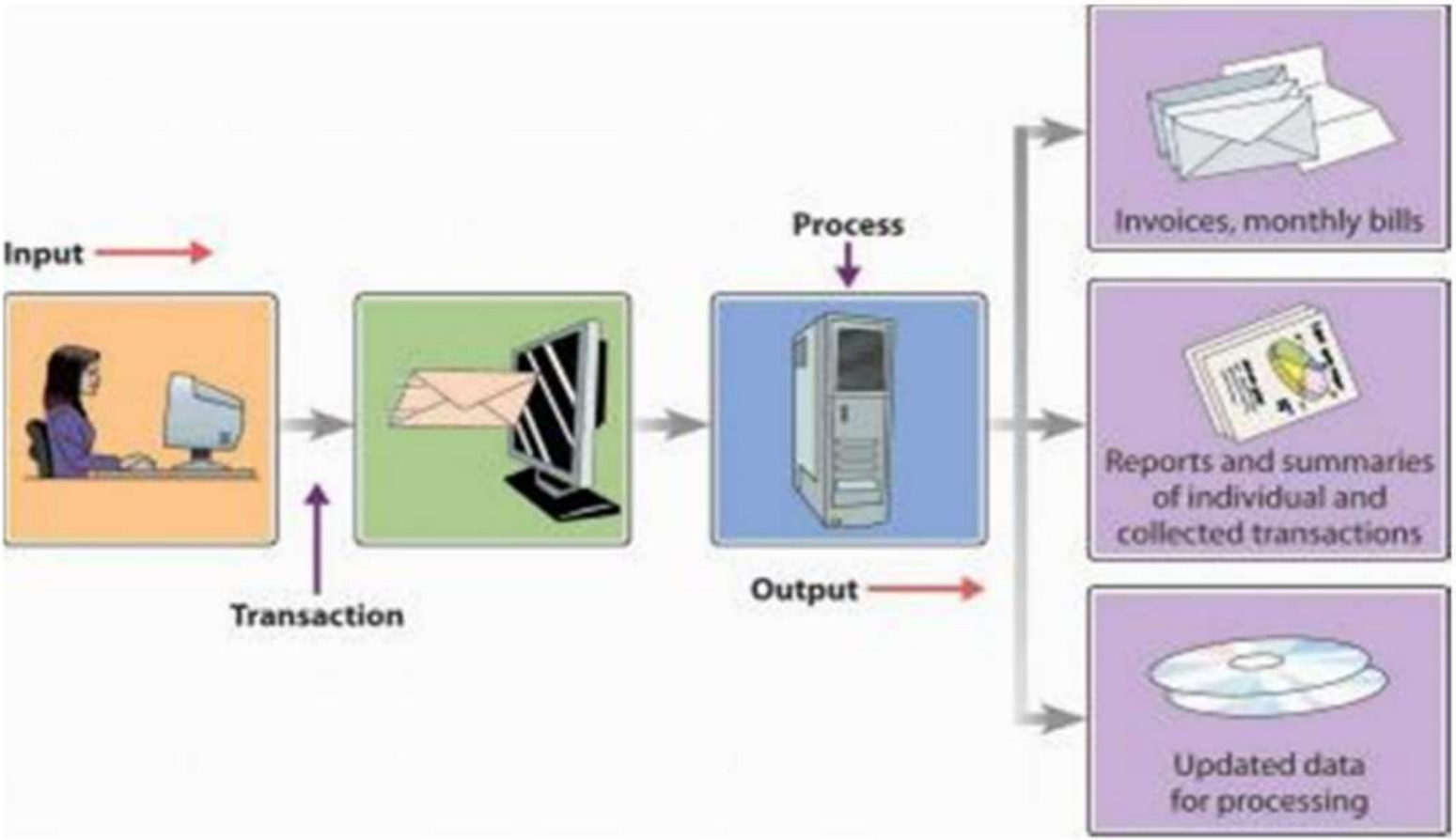
Transaction processing system

The main purpose of **Transaction Processing System** to fulfill the basic needs of record keeping of an organization.

Example

- Payroll System
- Billing Systems
- Purchasing System
- Shipping of record

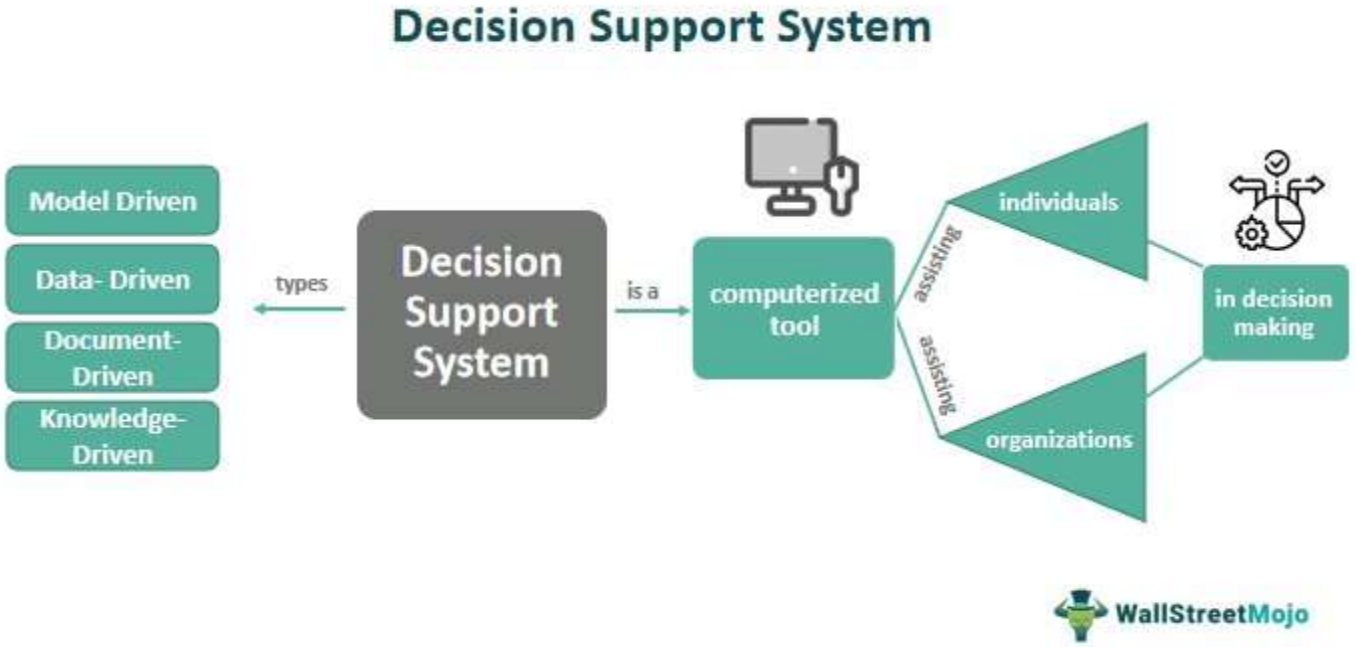
Its data is used for report generation. These can be monthly, quarterly or yearly reports or any on demand reports depending upon the needs of organization. Transaction Process System deals with routine transactions effectively.


Input
Process
Invoices, monthly bills
Reports and summaries of individual and collected transactions
Transaction
Output
Updated data for processing

Decision support system

- Decision Support System analyze the data which is used in decision making by the management of the organization. Data can be from internal or external sources. For example, if the management needs to asses the prices of a product, may use data from external sources i.e. market prices.

- DSS comes in a way when the data is more complex and is required in decision making. It helps the decision-makers to in a process of decision making. It may also involve databases and spreadsheets, complex in nature, for creating models in difficult and important situations.


Decision Support System
Model Driven
Data- Driven
Document-Driven
Knowledge-Driven
types
Decision Support System
is a
computerized tool
assisting
individuals
assisting
organizations
in decision making
WallStreetMojo

Executive information system

- Executive Information System also known as Executive Support System. It is developed for the Senior Management of the organization. It helps them to analyze the trends by viewing various reports including summaries; and then making the strategic decisions for the business.

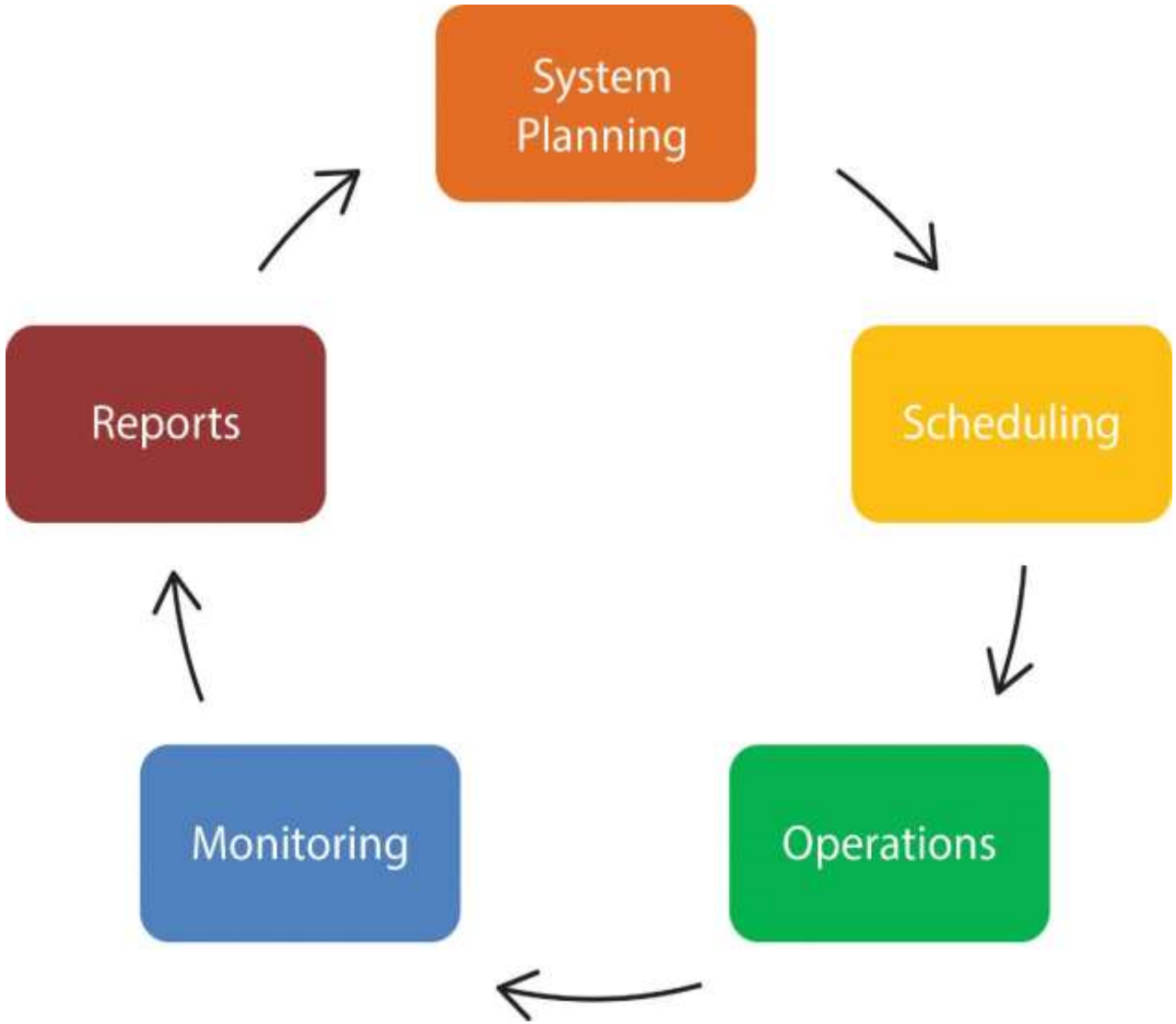
- These kinds of systems are easy to use and have many kind of reports specially, graphical type reports. The reports are prepared from large sets of data collected from various sources.

- For example, the management may require data of sales of the organizations that may be department wise or product wise ranging over a specific period. The system also include information about inventory, assets and revenue either collected or projected.

EXECUTIVE INFORMATION SYSTEM

Management information system

- Management Information System is also used by the management, but it differs from the Transaction Processing System (TPS) in a way that it provides summaries of routine nature to the management.
- The different kinds of data including sales, purchase, production is consolidated in MIS. Usually, this data is collected from internal sources. Summaries are prepared from this data used by managers and decision makers. This system can also support the marketing and revenue departments to enhance the operational efficiency and tracking the progress of the organization.


System Planning
Scheduling
Operations
Monitoring
Reports

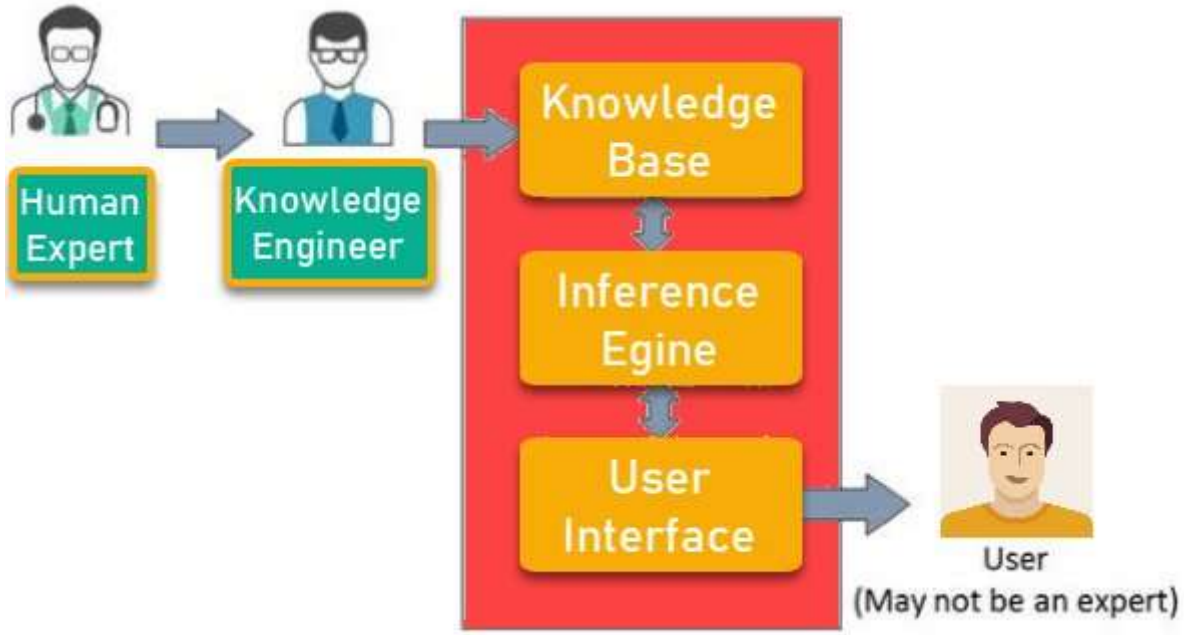
Enterprise resource planning

- Enterprise Resource Planning ERP is a system which revolves around the whole business process and has different integrated modules. Each module deals with different department. ERP systems are used by the multi-national organizations.


Enterprise Resource Planning
01
Human Resource Management
02
Customer Relationship Management
03
Financial Resource Management
04
Manufacturing Resource Management
05
Supply Chain Management
www.erp-information.com

Expert systems.

- The organizations use the expert systems to obtain suggestions as these systems acts like the experts and have ability to solve complex problems.
- Expert Systems were firstly started in 1970s. It is composed of inference engine *(it has logical set of rules which applied to knowledge base)* and knowledge base *(used to store structured and unstructured data — facts and rules)*.
- The example of knowledge base systems is Expert System. These play important role in many organizations.

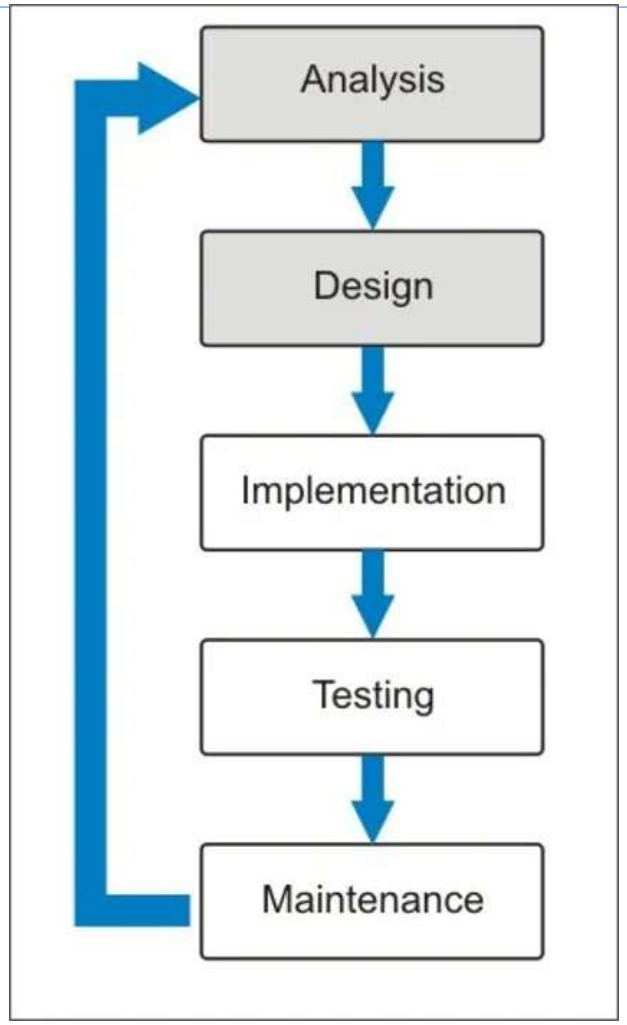

Human Expert
Knowledge Engineer
Knowledge Base
Inference Egine
User Interface
User
(May not be an expert)

Why Expert System

- No emotion
- High Efficiency
- Expertise in a domain
- No Memory limitation
- Regular updates improve the performance
- High Security
- Considers all facts

Development of information system


Analysis
Design
Implementation
Maintenance
Planning
System Development Life Cycle


Analysis
Design
Implementation
Testing
Maintenance

Development Information System?

System Survey
The SLDC phase also consists of three main points: system identification, selection, and system planning.
1) System Identification
This process is to identify the problems facing the company and the system it has. The team will look for any opportunities that can be done to overcome this.

2) Selection
The selection phase will apply evaluation points to the development project to ensure the solutions are created in accordance with the company's expected targets.

Cont…

3) System Planning

This step is the step of developing a formal plan to start working on and implementing the information system development concept that has been chosen.

Analysis

- System requirements analysis is a technique for solving problems by decomposing the components of the system. The aim is none other than to find out more about how each component works and the interaction between one component with other components.

- Some aspects that need to be targeted in the needs analysis in the development of information systems include business users, job analysis, business processes, agreed rules, problems and solutions, business tools, and business plans.

Design

- The design or design of system development is intended to provide a complete blueprint as a guideline for the IT team (especially programmers) in making applications. Thus the IT team no longer makes decisions or works in a sporadic way.

Implementation

- This phase is less creative than system design. It is primarily concerned with user training, site preparation, and file conversion. When the candidate system is linked to terminals and remote sites the telecommunication network and tests of the network along with the system are also included under implementation.

- During the final testing, user acceptance is tested, followed by user training. Depending on the nature of the system, extensive user training may be required, conversion usually takes place at about the same time the user is being trained or later.

Testing

- A system needs to be tested to ensure that the development carried out is appropriate or not with the expected results. Tests that are applied are various, such as performance, input efficiency, syntax (program logic), output, and so on.

- This information system development stage requires preparation of various supporting aspects. In addition to applications, hardware readiness and several other related facilities also need to be prepared. As for implementation, several activities carried out include data migration (conversion), training for users, and trials.

Change and Maintenance

- This step covers the whole process in order to ensure the continuity, smoothness and improvement of the system. In addition to monitoring the system at a certain time, maintenance also includes activities to anticipate minor bugs (bugs), system improvements, and anticipation of some risks from factors outside the system.

What is Information Security?

- Information security is “the state of the well-being of information and infrastructure in which the possibility of theft, tampering, or disruption of information and services is kept low or tolerable.”

OR

- Information security refers to the protection or safeguarding of information and information systems that use, store, and transmit information from unauthorized access, disclosure, alteration, and destruction.

- Information Security is the protection of the information available in the electronic systems and physical form.
- Infosec deals with information, regardless of its format (it encompasses paper documents, digital and intellectual property in people's minds, and verbal or visual communications.

What is Information Security?

- Information security, sometimes shortened to **InfoSec**, is the practice of protecting information by mitigating information risks. It is part of information risk management.

OR

- Information security refers to the protection or safeguarding of information and information
  systems that use, store, and transmit information from unauthorized access, disclosure, alteration, and destruction.

What is Data and Information?

- **Data** is a collection of raw, unorganized facts and details like text, observations, figures, symbols and descriptions of things etc.
- In other words, data does not carry any specific purpose and has no significance by itself. Moreover, data is measured in terms of bits and bytes – which are basic units of information in the context of computer storage and processing.

- **Information** is processed, organized and structured data. It provides context for data and enables decision making. For example, a single customer's sale at a restaurant is data – this becomes information when the business is able to identify the most popular or least popular dish.

Difference between data and information?

Data	Information
Data is unorganized and unrefined facts	Information comprises processed, organized data presented in a meaningful context
Data is an individual unit that contains raw materials which do not carry any specific meaning.	Information is a group of data that collectively carries a logical meaning.
Data doesn't depend on information.	Information depends on data.
Raw data alone is insufficient for decision making	Information is sufficient for decision making
An example of data is a student's test score	The average score of a class is the information derived from the given data.

Difference between Cybersecurity & Information Security

Cybersecurity?

- Network Security
- Application Security
- Cloud Security
- Critical Infrastructure

Information Security?

- Inclusive of Cybersecurity &..
- Procedural Controls
- Access Controls
- Technical Controls
- Compliance Controls

Difference between Cybersecurity & Information Security

Parameters	CYBER SECURITY	INFORMATION SECURITY
Basic Definition	It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity, and availability.
Protect	It is about the ability to protect the use of cyberspace from cyber-attacks.	It deals with the protection of data from any form of threat.
Scope	Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.
Threat	Cybersecurity deals with the danger in cyberspace.	Information security deals with the protection of data from any form of threat.
Attacks	Cybersecurity strikes against Cyber-crimes, cyber frauds, and law enforcement.	Information security strikes against unauthorized access, disclosure modification, and disruption.
Professionals	Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).	Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and availability.
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.
Defense	Acts as first line of defense.	Comes into play when security is breached.

Need for Information security

- **Confidentiality:**
  Protecting the confidentiality of sensitive information is paramount. Information security measures ensure that only authorized individuals or systems have access to confidential data, preventing unauthorized disclosure.

- **Integrity:**
  Information integrity ensures that data remains accurate, consistent, and unaltered. Security measures help prevent unauthorized modifications or tampering, maintaining the reliability of information.

- **Availability:**
  Information security safeguards are crucial to ensuring that information and information systems are available when needed. This includes protecting against disruptions, such as cyberattacks, natural disasters, or technical failures.

Need for Information security

- **Prevention of Unauthorized Access:**
  Information security measures, including strong authentication and access controls, help prevent unauthorized individuals from gaining access to sensitive data or critical systems.

- **Protection Against Cyber Threats:**
  The digital landscape is fraught with various cyber threats, including malware, phishing attacks, ransomware, and more. Information security practices are essential for identifying, preventing, and mitigating these threats.

- **Compliance with Regulations:**
  Many industries and jurisdictions have specific regulations and compliance requirements regarding the protection of sensitive information. Adhering to these regulations is not only a legal obligation but also essential for maintaining trust with customers and stakeholders.

Need for Information security

Business Continuity:

- Information security is integral to business continuity planning. By safeguarding critical systems and data, organizations can recover more swiftly from disruptions, minimizing downtime and associated financial losses.

Personal Privacy:

- Individuals entrust organizations with their personal information. Information security is necessary to protect the privacy of individuals by preventing unauthorized access and misuse of personal data.

Protection of Reputation:

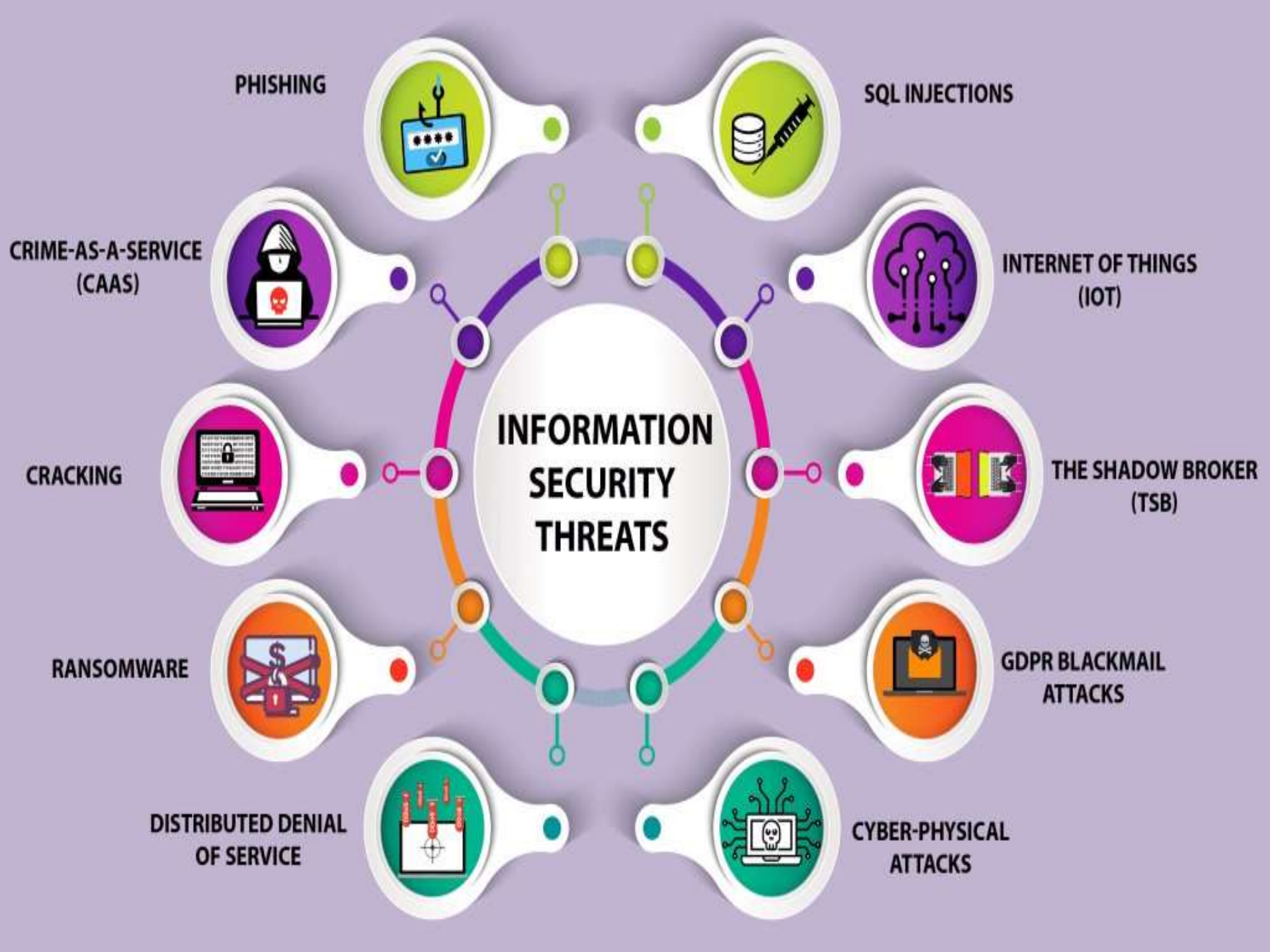
- A breach of information security can severely damage an organization's reputation. Maintaining the trust of customers, partners, and the public is crucial for long-term success, and information security is a key component of building and preserving that trust.

Prevention of Financial Loss:

- Cybersecurity incidents can lead to significant financial losses, including costs related to system restoration, legal actions, and the potential loss of business. Information security measures help mitigate these financial risks.

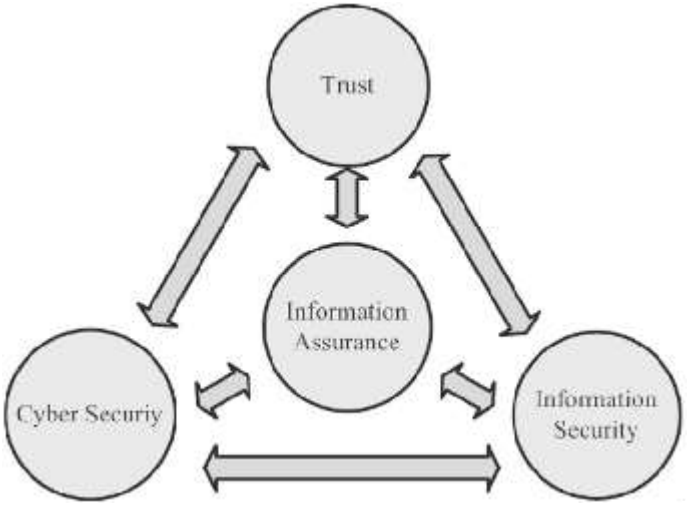
Threats to Computerized Information Systems

- Hardware failure
- Software failure
- Personnel actions
- Terminal access penetration
- Theft of data, services, equipment
- Fire
- Electrical problems
- User errors
- Unauthorized program changes
- Telecommunication problems


INFORMATION SECURITY THREATS
PHISHING
SQL INJECTIONS
CRIME-AS-A-SERVICE (CAAS)
INTERNET OF THINGS (IOT)
CRACKING
THE SHADOW BROKER (TSB)
RANSOMWARE
GDPR BLACKMAIL ATTACKS
DISTRIBUTED DENIAL OF SERVICE
CYBER-PHYSICAL ATTACKS

What is information assurance?

- *Information assurance (IA) is the practice of assuring information and managing risks related to the use, processing, storage and transmission of information. Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data.*



Information assurance?

- IA focuses on risk management and produces guidelines for keeping information secure, whether on physical (hard drives, PCs, laptops and tablets) or digital (cloud) systems. Cybersecurity focuses on setting up resilient network architecture to secure digital assets from unwarranted access.
- IA is concerned with the business aspect of information. As a result, the scope is broader. Cybersecurity deals in the nitty-gritty to protect everything. As a result, the scope is more detailed.

Approach?

- IA is strategic, dealing with policy creation and deployment to keep information assets secure. It understands how an organization engages with information, the value of the information and how exposed that information happens to be. Cybersecurity is technical, dealing with security controls and tools to defend against cyberattacks.

Goal of information assurance?

The purpose of IA is to reduce information risks by ensuring the information on which the business makes decisions is reliable. This purpose is achieved by following:

Risk management: Businesses face legal fines and penalties if the information in the network is compromised. IA enables risk assessment to identify vulnerabilities and the potential impact on the business in terms of compliance, cost and operational continuity. The goal is to mitigate potential threats.

Encryption at rest and in transit: IA mandates end-to-end encryption to protect privacy by ensuring no human or computer can read data at rest and in transit except the intended parties. The goal is to help businesses stay compliant with regulatory requirements and standards.

Data integrity: Bad business decisions usually stem from bad data. IA focuses on auditing data collection and tracking process, improving transparency in the organizational process. The goal is to manage data in a way that a future audit can retrace the process, leading to better decision-making.

need of information assurance?

Operational benefits:

Resilient business processes
Improved customer service
Better information usage
Improved responsiveness

Strategic benefits:

Better governance
Cheaper equity
More sales
Lower costs

Organizational benefits:

Improved shareholder value
Gain competitive advantage
License to operate

What is Cyber Security?

- Cybersecurity is the state or process of protecting and recovering computer systems, networks, devices, and programs from any type of cyber-attack. Cyber-attacks are an increasingly sophisticated and evolving danger to your sensitive data, as attackers employ new methods powered by social engineering and artificial intelligence (AI) to circumvent traditional data security controls.

OR

- Cybersecurity is the practice of securing system devices, network and data that are in the electronic form/ systems.

Need for Cybersecurity

Cybersecurity is important because it protects all categories of data from theft and damage.

- Evolution of technology, focused on ease of use
- Rely on the use of computers for accessing, providing, or just storing information
- Increased network environment and network-based applications
- Direct impact of security breach on the corporate asset base and goodwill
- Increasing complexity of computer infrastructure administration and management

Need for Cybersecurity

- **Rising Cyber Threats:** The proliferation of cyber threats poses a growing risk to the security and integrity of digital systems and data.
- **Intellectual Property Protection:** Safeguarding intellectual property is crucial due to the risk of cyberattacks leading to IP theft or compromise.
- **Disruption of Operations:** Cybersecurity incidents can disrupt business operations, causing downtime and productivity loss.
- **Human Error Vulnerabilities:** Human mistakes play a significant role in cybersecurity incidents, highlighting the importance of training and awareness.
- **Reputation Damage:** Cybersecurity breaches can severely damage an individual's or organization's reputation and trustworthiness in the eyes of the public.

Need for Cybersecurity

- **Economic Costs:** Theft of intellectual property, corporate information, disruption in trading, and the cost of repairing damaged systems.
- **Regulatory Costs:** GDPR and other data breach laws mean that your organization could suffer from regulatory fines or sanctions as a result of cybercrimes.
- **Supply Chain Vulnerabilities:** Organizations are interconnected through supply chains, and a breach in one organization can affect others in the chain, causing a ripple effect.

Cyber security risk analysis?

- **Asset Identification:**
  Identify and catalog all digital assets within the organization, including hardware, software, data, networks, and personnel.

- **Threat Identification:**
  Identify potential threats and vulnerabilities that could exploit weaknesses in the organization's cybersecurity posture. This includes external threats (e.g., hackers, malware) and internal threats (e.g., insider threats).

- **Vulnerability Assessment:**
  Conduct a systematic evaluation of the organization's systems and networks to identify vulnerabilities. This may involve using automated tools, penetration testing, and other techniques.

- **Likelihood Assessment:**
  Assess the likelihood of each identified threat exploiting vulnerabilities. Consider factors such as historical data, threat intelligence, and the organization's security controls.

Cybersecurity risk analysis?

- **Documentation and Reporting:**
  Document the entire risk analysis process, including the identified risks, assessments, mitigation strategies, and residual risks. Provide clear and concise reports for stakeholders.

- **Continuous Monitoring and Review:**
  Regularly monitor the cybersecurity landscape, update risk assessments as needed, and adapt mitigation strategies to address emerging threats and changes in the organization's IT environment.

Cybersecurity risk analysis?

- **Impact Assessment:**
  Evaluate the potential impact of a cybersecurity incident on the organization's assets, operations, reputation, and financial standing. Consider both tangible and intangible consequences.

- **Risk Calculation:**

Calculate the overall risk for each identified threat by combining the likelihood and impact assessments. This may involve assigning numerical values or qualitative ratings to different risk levels.

- **Risk Prioritization:**
  Prioritize risks based on their calculated risk levels. This helps organizations focus their resources on addressing the most significant and potentially damaging threats.

- **Mitigation Strategies:**

Develop and implement strategies to mitigate or reduce identified risks. This may involve implementing security controls, improving security awareness, updating software, or enhancing incident response capabilities.


01
Identify
02
Assess &
Evaluate
03
Strategize
04
Implement
05
Monitor &
Document
Risk Control
Cycle

1. https://www.scribd.com/document/77460357/Introduction-of-Information-System

2. https://deden08m.files.wordpress.com/2011/03/ch01-introduction-to-information-systems.pdf

3. https://ecampusontario.pressbooks.pub/infosysbus/chapter/chapter-1-what-is-an-information-system/

4. https://bbamantra.com/introduction-information-system/
5. https://limeproxies.netlify.app/blog/top-10-information-security-threats-in-2018

Parul® University

NAAC GRADE A++

https://paruluniversity.ac.in/