Unit-4

Ethical Issues Pertaining to IS

Prof. Suhag Baldaniya

✓ Topics

- Ethical responsibilities of business professionals
- Computer crime - Hacking and cracking, Cyber theft, Unauthorized use at work, Software piracy, Theft of intellectual property, Viruses and worms, Adware, and Spyware.
- The first line of defense – People/employees
- The Second line of defense – Technology for authorization, prevention, detection, and response
- Choice of Information Technology.

Ethical Responsibilities of Business Professionals

Meaning of Ethics

- The word "ethics" is derived from the Greek word **ethos** (character), and the Latin word **mores (customs).** In the legal context, ethics defines how individuals choose to interact with one another.
- According to Crane, "**Business ethics is the study of business situations, activities, and decisions where issues of right and wrong are addressed**."
- Baumhart defines, **"The ethics of business is the ethics of responsibility. The business man must promise that he will not harm knowingly."**

Business Ethics

- Business ethics are **policies that guide the behavior of corporate entities, especially regarding controversial subjects.**
- Business ethics **protect companies from legal liability** and **ensure that they treat their customers and team members with respect**.
- Corporate ethics codes often include subjects like **social responsibility, insider trading, discrimination, corporate governance, and bribery.**
- The purpose of business ethics is **to ensure a consistent moral attitude within the company, from executive-level management to the new hire.**
- Business ethics helps to ensure everyone in a workplace is treated with respect, fairness and honesty.

Need & Importance of Business Ethics in the Workplace

- **Reputation and Trust**
  - **Importance:** Ethical behavior builds a positive reputation for a business, fostering trust among customers, employees, investors, and other stakeholders.
  - **Impact:** A good reputation attracts customers, retains talented employees, and enhances brand value, ultimately contributing to long-term success.
- **Customer Loyalty**
  - **Importance:** Customers prefer to engage with businesses that demonstrate ethical behavior.
  - **Impact:** Ethical practices, such as fair pricing, honest advertising, and quality products/services, contribute to customer satisfaction and loyalty.

Need & Importance of Business Ethics in the Workplace

- **Employee Morale and Productivity**
  - **Importance:** Ethical treatment of employees creates a positive work environment, boosting morale and job satisfaction.
  - **Impact:** Satisfied and motivated employees are more likely to be productive, innovative, and committed to the success of the organization.
- **Legal Compliance**
  - Importance: Adherence to ethical standards ensures compliance with laws and regulations.
  - Impact: Avoiding legal issues and penalties protects the business from financial losses and reputational damage.

Need & Importance of Business Ethics in the Workplace

- **Investor Confidence**
  - **Importance:** Ethical behavior enhances the confidence of investors and shareholders.
  - **Impact:** Investors are more likely to support and invest in companies that are transparent, trustworthy, and committed to ethical business practices.
- **Competitive Advantage**
  - **Importance:** Ethical practices can differentiate a business from its competitors.
  - **Impact:** Consumers increasingly prefer businesses with a social conscience, giving ethically-driven companies a competitive edge in the market.

Need & Importance of Business Ethics in the Workplace

- **Global Operations and Reputation**
  - **Importance:** In an interconnected world, news about unethical practices can spread rapidly.
  - **Impact:** International businesses must adhere to ethical standards to avoid damaging their global reputation, ensuring acceptance in diverse markets.
- **Long-Term Sustainability**
  - **Importance:** Ethical behavior is essential for the long-term sustainability of a business.
  - **Impact:** Sustainable business practices, social responsibility, and ethical decision-making contribute to environmental and social well-being, aligning with changing societal expectations.

Need & Importance of Business Ethics in the Workplace

- **Customer and Employee Relations**
  - **Importance:** Ethical conduct strengthens relationships with both customers and employees.
  - **Impact:** Positive relationships lead to repeat business, customer loyalty, and a stable, committed workforce.
- **Risk Management**
  - **Importance:** Ethical decision-making helps in identifying and mitigating risks.
  - **Impact:** Businesses that integrate ethical considerations into decision-making are better equipped to anticipate and manage potential risks, minimizing negative consequences.

Need & Importance of Business Ethics in the Workplace

- **Public Perception and Brand Image**
  - **Importance:** Ethical behavior influences public perception and brand image.
  - **Impact:** A positive public perception enhances the overall image of the brand, attracting customers and stakeholders who value ethical practices.
- **Social Responsibility**
  - **Importance:** Businesses play a crucial role in contributing to the well-being of society.
  - **Impact:** Ethical business practices demonstrate a commitment to social responsibility, addressing societal issues and contributing to the greater good.

Ethical Issues in Business

- Ethical issues in business occur **when a decision, activity or scenario conflicts with the organization’s or society's ethical standards.**
- Both organizations and individuals can **become involved in ethical issues since others may question their actions from a moral viewpoint.**
- Ethical conflicts may **pose a risk for an organization**, as they may imply non-compliance with relevant legislation.
- In other instances, ethical issues may **not have legal consequences but may cause an adverse reaction from third parties**. It may be **challenging to effectively manage ethical issues when no guidelines exist**.
- For this reason, as an HR or management professional, you can help develop policies to guide employees to make the right decision when faced with moral issues.

Ethical Issues in Business

- **Discrimination and harassment**
  - The consequences of discrimination and harassment in the workplace can negatively impact the finances and reputation of the organization. Some anti-discrimination areas include:
    - **Age**
    - **Disability**
    - **Equal pay**
    - **Pregnancy**
    - **Race**
    - **Religion**
    - **Gender**

Ethical Issues in Business

- **Workplace health and safety**
  - All employees have a right to a safe working environment and work conditions. Some of the most common employee safety considerations include,
    - **Hazard communication**
    - **Respiratory protection**
    - **Electrical wiring methods**
    - **Machine guarding**
- **Whistle-blowing or social media rants**
  - Using social media has become widespread, making employees' online conduct a critical consideration in their employment status.
  - The consequences of punishing employees for inappropriate social media posts remains an ethical issue, and the implications of a negative social media post may influence the treatment of the employee.

Ethical Issues in Business

- **Ethics in accounting practices**
  - Laws require organizations to maintain accurate bookkeeping practices. Unethical accounting practices are a serious issue, especially for publicly traded companies.
- **Corporate espionage and nondisclosure**
  - Many organizations are at risk that current and former employees may steal information, such as client data, for use by competitors.
  - Stealing an organization's intellectual property or illegally distributing private client information constitutes corporate espionage. This is why it can be helpful to require mandatory nondisclosure agreements.

Ethical Issues in Business

- **Technology and privacy practices**
  - Developments in an organization’s technological security capabilities may pose privacy concerns for both employees and clients.
  - Electronic surveillance includes monitoring Internet connections and tracking keystrokes, content, or time spent using the keyboard. When implementing these types of surveillance, you can act ethically by being transparent about it with employees.
- **Nepotism or favouritism**
  - You may want to employ an acquaintance or family member because of your connection to them. Even if you adhere to recruitment policies to ensure a fair process, some employees may still consider this as nepotism or favoritism.

Ethical Issues in Business

- **Environmental responsibility**
  - Many organizations are increasing corporate social responsibility activities.
  - You can help create policies that ensure the organization you work for acts in a responsible way towards employees, the community and the environment.
  - If you work for a smaller organization, you may wish to reduce the company's impact on air and water quality.

Ethical Responsibility of Business Professional

- **Integrity and Honesty**
  - Business professionals should maintain honesty and integrity in all their dealings. This includes being truthful in communication, providing accurate information, and avoiding deceptive practices.
- **Fairness and Equity**
  - Professionals should treat all stakeholders fairly and equitably. This involves avoiding discrimination, favoritism, and ensuring that decisions and actions are just and impartial.
- **Transparency**
  - Transparency involves being open and honest about business practices, financial dealings, and decision-making processes. This helps build trust among stakeholders, including customers, employees, and investors.

Ethical Responsibility of Business Professional

- **Respect for Stakeholders**
  - Business professionals have a responsibility to respect the rights and dignity of all stakeholders, including employees, customers, suppliers, and the community. This involves considering the impact of business decisions on various groups and addressing their concerns.
- **Compliance with Laws and Regulations**
  - Professionals must adhere to all applicable laws and regulations governing their industry and operations. This includes understanding and complying with legal requirements related to business practices, environmental impact, labor laws, and more.
- **Corporate Social Responsibility (CSR)**
  - Embracing CSR involves taking responsibility for the social and environmental impact of business activities. This may include initiatives related to sustainability, philanthropy, and community development.

Ethical Responsibility of Business Professional

- **Conflicts of Interest**
  - Professionals should avoid situations where personal interests conflict with the interests of the organization or its stakeholders. This includes disclosing potential conflicts and taking steps to mitigate them.
- **Professional Competence**
  - Business professionals have a responsibility to maintain and enhance their professional competence. This involves staying current with industry trends, continuously improving skills, and ensuring that decisions are based on a solid understanding of the relevant issues.
- **Whistleblowing**
  - Professionals should be encouraged to report unethical practices within the organization without fear of retaliation. Whistleblowing mechanisms help maintain accountability and prevent misconduct.

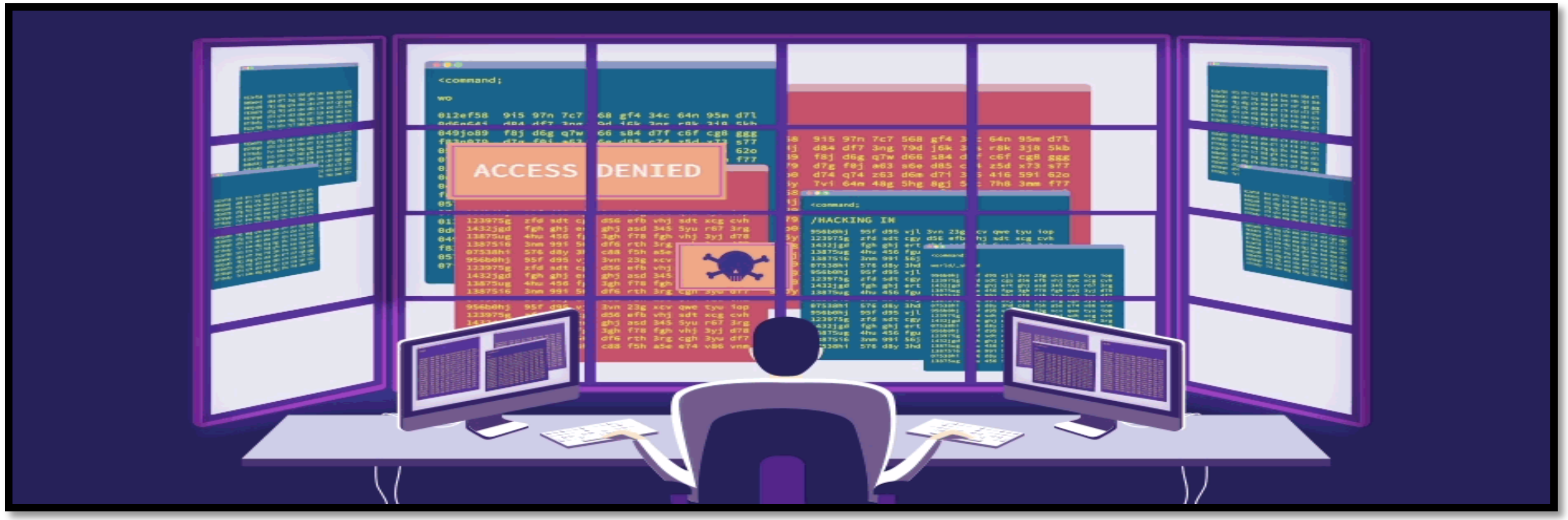
Ethical Responsibility of Business Professional

- **Environmental Responsibility**
  - Businesses should consider the environmental impact of their operations and strive to minimize their ecological footprint. This includes sustainable practices, energy efficiency, and responsible resource management.

Introduction to Computer Crime

Computer Crime

- The term "cybercrime" was **introduced after the latest evolution in the computer industry and networks.**
- Cybercrimes are considered a major risk because they can **have devastating effects like financial losses, breaches of sensitive data, and failure of systems, and also, can affect an organization's reputation.**
- Cybercrime can be defined as **"The illegal usage of any communication device to commit or facilitate in committing any illegal act".**



Computer Crime

- A cybercrime is explained as **a type of crime that targets or uses a computer or a group of computers under one network to harm.**
- They can be **targeting individuals, business groups, or even governments.**

Hacking and Cracking

Cyber Theft

Unauthorised Use at Work

Software Piracy

Theft of Intellectual Property

Virus and Worms

Adware & Malware

Hacking

- Hacking has been **a part of computing for almost five decades** and it is a very **broad discipline, which covers a wide range of topics.**
- The first known event of hacking had taken place in **1960 at MIT** and at the same time, the term "Hacker" was originated.
- Hacking is the act of finding the **possible entry points** that exist in a computer system or a computer network and finally entering into them.
- Hacking is usually done to gain **unauthorized access** to a computer system or a computer network, either **to harm the systems or to steal sensitive information** available on the computer.

Hacking

- Hacking is usually **legal as long as it is being done to find weaknesses in a computer or network system for testing purposes**. This sort of hacking is what we call **Ethical Hacking.**
- A computer expert who does the act of hacking is called a **"Hacker"**.
- Hackers are those who seek knowledge, to understand how systems operate, and how they are designed, and then attempt to play with these systems.

Types of Hacking

Website Hacking

- Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.

Network Hacking

- Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.

Email Hacking

- It includes getting unauthorized access to an Email account and using it without obtaining the consent of its owner.

Types of Hacking

Ethical Hacking

- Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.

Computer Hacking

- This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

Password Hacking

- This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.

Advantages of Hacking

- Hacking is quite useful in the following scenarios –
- To **recover** lost information, especially in case you lost your password.
- To perform penetration **testing** to strengthen computer and **network security**.
- To put adequate **preventative** measures in place to prevent security breaches.
- To have a computer system that **prevents malicious** hackers from gaining access.

Disadvantages of Hacking

- Hacking is quite **dangerous** if it is done with harmful intent.
- It can cause – Massive **security** breach.
- **Unauthorized** system access on private information.
- **Privacy** violation.
- **Hampering** system operation.
- Can not denial of **service attacks**.
- Malicious **attack** on the system.

Cracking

- Cracking is when **someone performs a security hack for criminal or malicious reasons**, and the person is called a “cracker.”
- Just like a bank robber cracks a safe by skillfully manipulating its lock, **a cracker breaks into a computer system, program, or account with the aid of their technical wizardry.**
- Hackers use their own legal tools for checking network strength, establishing security, and protecting an organization from internet threats.
- Crackers **don't have any tools of their own**. They make **use of someone else's tools** to perform illegal activities and harming/compromise a system.

Unauthorised Use at Work

- The unauthorized use of **computer systems and networks** can be called time and resource theft.
- A common example is the **unauthorized use of company-owned computer networks by employees.**
- This may range from **doing private consulting or personal finances or playing video games** to unauthorized use of the internet on company networks.
- Network monitoring software called ‘**sniffers**’ is frequently used to monitor network traffic to evaluate network capacity as well as reveal **evidence** of **improper use**.
- According to one survey, 90% of United States workers admit to surfing **recreational sites** during office hours, and 84% say they send personal E-mails from work.

Software Piracy

- Software piracy is **the act of illegally using, copying, modifying, distributing, sharing, or selling computer software** protected by copyright laws.
- A software pirate is **anyone who intentionally or unintentionally commits** these illegal acts.
- The end-user license agreement (EULA) is the most common license for software protection. It is a legal contract between the software manufacturer (or author) and the end-user (or customer) that defines the rules of the software use.
  - Example:
    - Purchasing a single-user license for a piece of software and downloading it on your own computer as well as on someone else’s computer.
    - Downloading copyrighted films, music, games, or e-books from shady websites for free.

Theft of Intellectual Property

- With the growth in the use of internet these days the cyber crimes are also growing.
- Cyber theft of Intellectual Property(IP) is one of them.
- Cyber theft of IP means stealing of **copyrights, trade secrets, patents** etc., using internet and computers.
- **Copyrights and trade secrets are the two forms of IP** that is frequently stolen.
  - For example, **stealing of software, a unique recipe of a well-known dish, business strategies**, etc.
- Generally, the stolen material is sold to rivals or others for further sale of the product.

Theft of Intellectual Property

- This may result in a **huge loss** to the company who created it.
- Earlier, a lot of **physical** labour, time and money was spent to steal a trade secret or make a pirated version of anything.
- The original copies had to be **physically stolen which used to take lot of time and money.**
- But in the present scenario these works can be done easily **sitting** at one place without shedding too much time and money on it **without leaving any proof** of it.

Theft of Intellectual Property

- One of the **major cyber theft of IP faced by India is piracy**. These days one can get pirated version of movies, software etc. The piracy results in a huge loss of revenue to the copyright holder.
- It is **difficult to find the cyber thieves and punish** them because everything they do is over internet, so they erase the data immediately and disappear within fraction of a second.
- The country has started taking strict measures to curb this offence. **Telangana Intellectual Property Crime Unit (TIPCU)** is one of the first unit that has been launched to deal with the IP crime.

TELANGANA STATE

INTELLECTUAL PROPERTY AWARDS

for IP Champions

Deadline: Friday, 24th April 2020

Powered by

CII

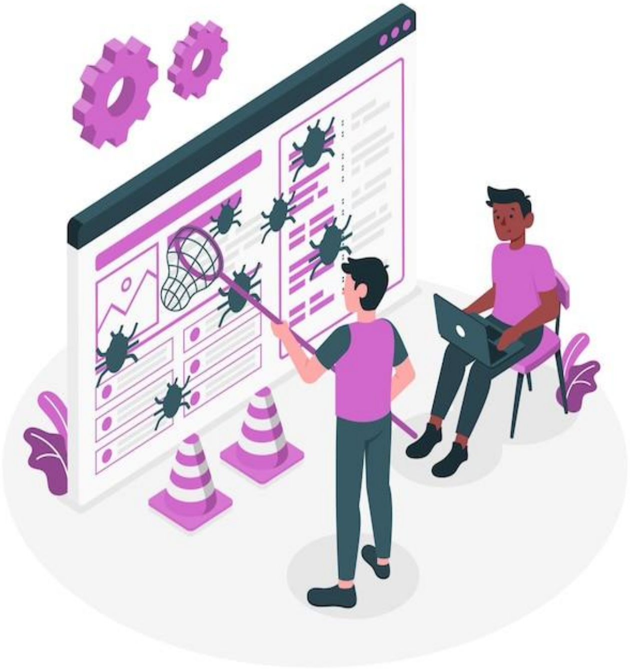
Outreach Partner

TELANGANA STATE

GLOBALLINKER

Virus

- A Virus is a **malicious executable code attached to another executable file** which can be harmless or can modify or delete data.
- The main objective of viruses is **to modify the information**.
- It requires host is needed for spreading.
- **Antivirus software** is used **for protection** against viruses.
- Viruses can’t be **controlled by remote**.
- Viruses are **executed via executable files.**
- Viruses generally **come from shared or downloaded files.**
- Examples of viruses include Creeper, Blaster, Slammer, etc.
- Its spreading **speed is slower as compared to worms**.



Virus

Symptoms

- Pop-up windows linking to malicious websites
- Hampering computer performance by slowing down it
- After booting, starting of unknown programs.
- Passwords get changed without your knowledge

Prevention

- Installation of Antivirus software
- Never open email attachments
- Avoid usage of pirated software
- Keep your operating system updated
- Keep your browser updated as old versions are vulnerable to linking to malicious websites

Warning Message
WARNING !
VIRUS DETECTED
Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat
CANCEL

Worms

- A **Worm is a form of malware** that replicates itself and **can spread to different computers via Network.**
- The main **objective of worms is to eat the system resources**.
- It consumes system resources such as **memory and bandwidth and makes the system slow** in speed to such an extent that it **stops responding**.
- It **doesn’t need a host to replicate from one computer to another.**
- It is **less harmful** as compared.
- Worms can be **detected and removed by the Antivirus and firewall.**

Worms

- Worms can be **controlled by remote**.
- Worms are **executed via weaknesses in the system.**
- Worms generally come from the **downloaded files or through a network connection.**
- Examples of worms include **Morris worm, storm worm,** etc.
- It does not need **human action to replicate**.
- Its spreading **speed is faster**.

Worms

Symptoms

- Hampering computer performance by slowing down it
- Automatic opening and running of programs
- Sending of emails without your knowledge
- Affected the performance of web browser
- Error messages concerning to system and operating system

Prevention

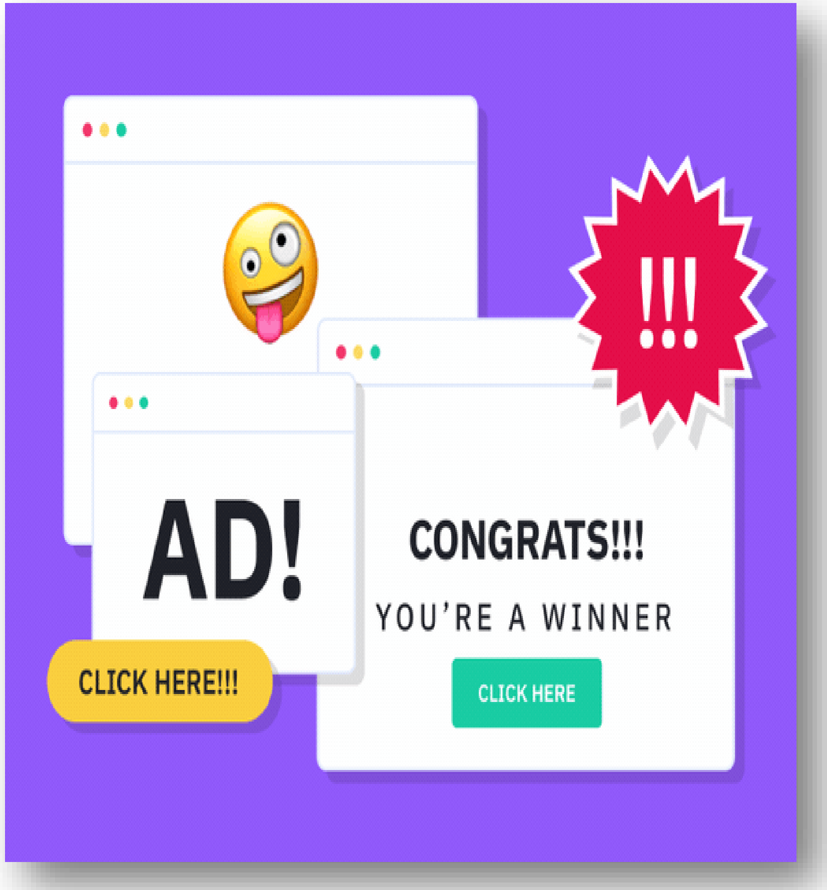
- Keep your operating system and system in updated state
- Avoid clicking on links from untrusted or unknown websites
- Avoid opening emails from unknown sources
- Use antivirus software and a firewall

Adware

- Adware and spyware are types of malicious software (malware) that are **designed to infiltrate and compromise computer systems** for various purposes.
- Adware, short for **advertising-supported software, is software that displays unwanted advertisements on a user's computer.**

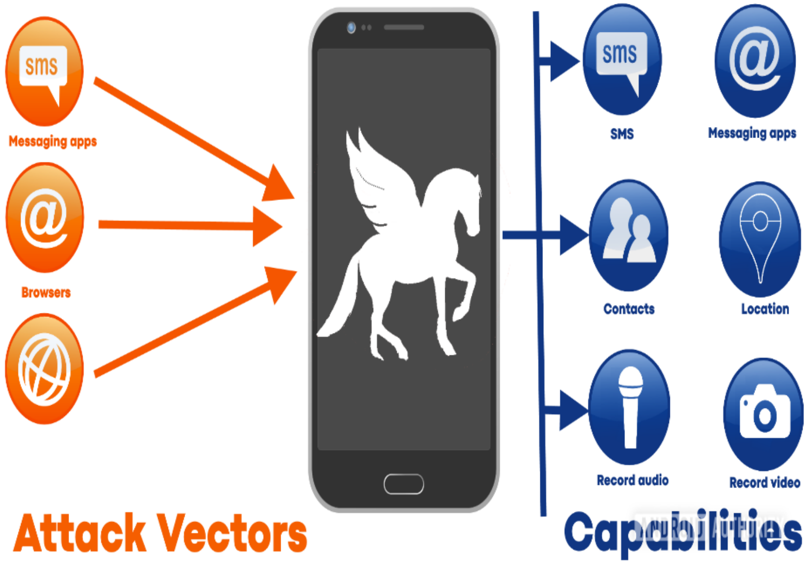
Adware

- The primary goal of adware is **to generate revenue for the creator by delivering advertisements, often in the form of pop-up ads or banners**, to the user.
  - **Example:** One example of adware is the **"Superfish"** adware that was pre-installed on certain Lenovo laptops.
  - Superfish injected third-party ads into web pages and also compromised the security of secure HTTPS connections by using a self-signed root certificate.
- While **adware is not always dangerous**, in some cases it may be designed **to analyze the Internet sites visited, present advertising content, install additional programs, and redirect your browser** to unsafe sites.



Spyware

- Pegasus is a **spyware developed by the Israeli cyber-arms company** NSO Group that is **designed to be covertly and remotely installed on mobile phones running iOS and Android.**
- While NSO Group markets Pegasus as a **product for fighting crime and terrorism, governments** around the world have routinely used the **spyware to surveil journalists, lawyers, political dissidents, and human rights activists.**
- Pegasus is **capable of reading text messages, tracking calls, collecting passwords, location tracking, accessing the target device's microphone and camera**, and harvesting information from apps.



Spyware

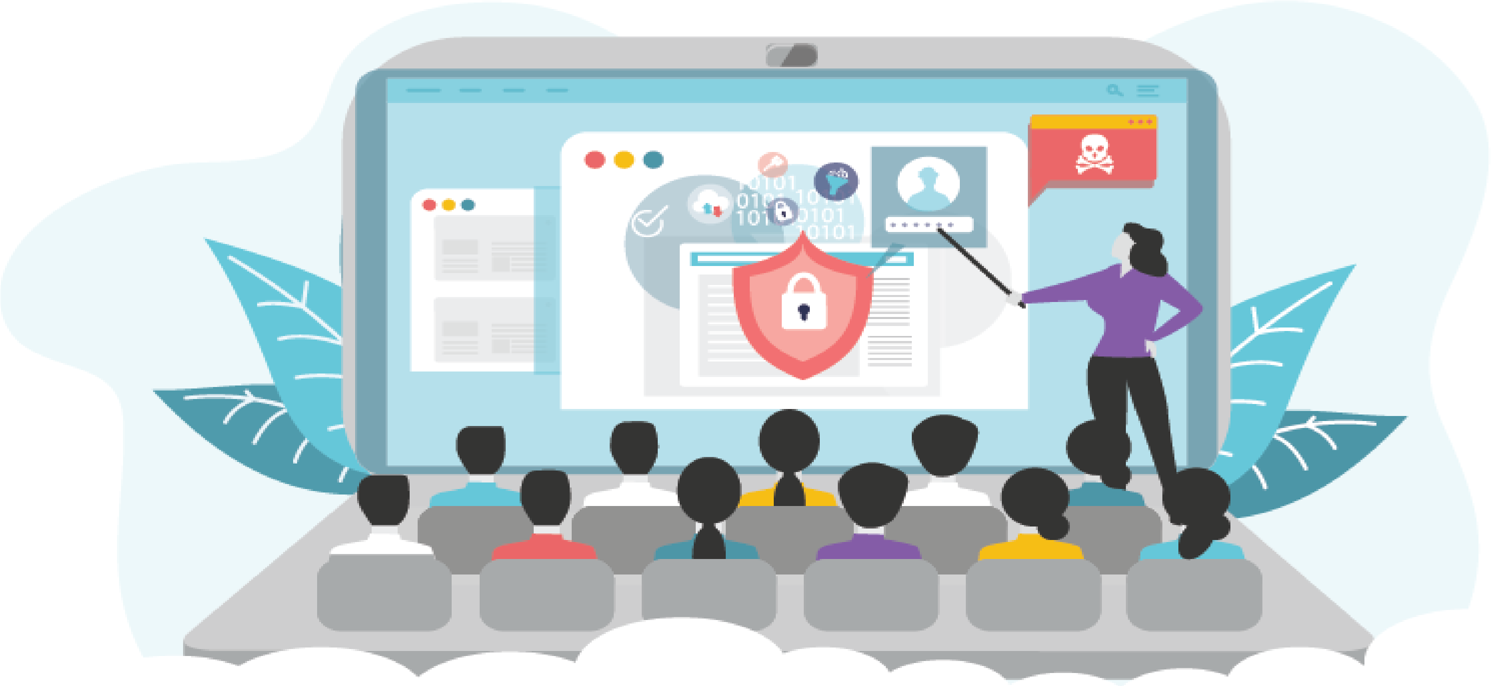
- Spyware is **a type of malware designed to secretly collect and transmit sensitive information** about a user's activities without their knowledge or consent.
- This information can include **keystrokes, browsing habits, login credentials, and personal data.**
  - **Example:** The "Zeus" Trojan is an example of spyware. Zeus, also known as Zbot, is a sophisticated Trojan horse that primarily targets financial information. It can capture login credentials for online banking and other sensitive data, sending it to remote servers controlled by cybercriminals.

Adware and Spyware

- It's important to note that adware and spyware can **sometimes overlap**, as certain adware may also collect user information.
- Additionally, both types of malware can be **delivered through deceptive practices, such as bundled software installations, misleading advertisements, or malicious email attachments.**
- To protect against adware, spyware, and other forms of malware, users should keep their **software up-to-date, use reputable antivirus and anti-malware programs**, be cautious when downloading and installing software, and avoid clicking on suspicious links or ads.
- Regularly **scanning your system for malware and practicing safe browsing habits** are essential for maintaining a secure computing environment.

The first line of defense in information system - People and Employee

- People and employees are **considered a crucial aspect of the first line of defense** in information systems.
- This includes **fostering a security-conscious culture among the workforce and ensuring that employees are aware** of and adhere to security policies and best practices.



Key Elements in First Line of Defense

- Security Training and Awareness
- User Authentication
- Employee Onboarding and Offboarding Processes
- Physical Security
- Security Policies and Procedures
- Incident Response and Reporting
- BYOD (Bring Your Own Device) Policies
- Security Mindset

Key Elements in First Line of Defense

- **Security Training and Awareness**
  - Regular training sessions to educate employees about security threats, phishing attacks, and best practices can significantly enhance the overall security posture.
- **User Authentication**
  - Ensuring that employees use strong, unique passwords and, when possible, implementing multi-factor authentication helps protect against unauthorized access.
- **Employee Onboarding and Offboarding Processes**
  - Proper procedures for granting and revoking access when employees join or leave the organization are critical to prevent unauthorized access.

Key Elements in First Line of Defense

- **Physical Security**
  - Securing physical access to servers, data centers, and other critical infrastructure is essential. This includes measures like access cards, biometric scanners, and surveillance.
- **Security Policies and Procedures**
  - Clearly defined security policies and procedures guide employees on how to handle sensitive information, use company resources securely, and report any security incidents promptly.
- **Incident Response and Reporting**
  - Employees should be aware of the procedures to follow in the event of a security incident. Prompt reporting can help mitigate potential damages.

Key Elements in First Line of Defense

- **BYOD (Bring Your Own Device) Policies**
  - If employees use personal devices for work, establishing and enforcing policies for secure usage is crucial to prevent potential vulnerabilities.
- **Security Mindset**
  - Encouraging a security mindset among employees involves cultivating a sense of responsibility for the security of the organization's information assets. This includes being cautious about clicking on suspicious links, using strong passwords, and reporting any security concerns.

The Second Line of Defense

- The second line of defense in an information system involves deploying **technology-based measures for authorization, prevention, detection, and response to enhance overall cybersecurity.**
- By implementing these technological measures, organizations can **fortify their defenses against a wide range of cyber threats, ensuring a more resilient and secure information system.**
- The second line of defense **complements the efforts of the first line (people and employees)** and forms a comprehensive approach to cybersecurity.

The Second Line of Defense

- Access Control Systems
- Firewalls
- Intrusion Prevention Systems (IPS)
- Antivirus and Anti-malware Solutions
- Data Encryption
- Security Information and Event Management (SIEM)
- Endpoint Protection
- Authentication Systems
- Vulnerability Management
- Incident Response Systems
- Network Segmentation

Key Elements in Second Line of Defense

- **Access Control Systems**
  - ↪ Utilizing advanced access control technologies to manage user permissions and privileges. This includes role-based access control (RBAC), where users are granted access based on their roles within the organization.
- **Firewalls**
  - ↪ Implementing firewalls to monitor and control incoming and outgoing network traffic based on predetermined security rules. Firewalls act as a barrier between a trusted internal network and untrusted external networks.
- **Intrusion Prevention Systems (IPS)**
  - ↪ Deploying systems that actively monitor network and/or system activities for malicious exploits or security policy violations. IPS can identify and block potential threats in real-time.

Key Elements in Second Line of Defense

- **Antivirus and Anti-malware Solutions**
  - Using software solutions to detect, prevent, and remove malicious software (malware) from systems. Regular updates to antivirus databases are essential to stay protected against evolving threats.
- **Data Encryption**
  - Employing encryption algorithms to secure sensitive data, both in transit and at rest. This adds an extra layer of protection, especially when data is being transferred over networks.
- **Security Information and Event Management (SIEM)**
  - Implementing SIEM solutions to collect, analyze, and correlate log data from various systems across the network. SIEM helps identify patterns indicative of security incidents.

Key Elements in Second Line of Defense

- **Endpoint Protection**
  - Utilizing security solutions to safeguard individual devices (endpoints) such as computers, laptops, and mobile devices. Endpoint protection includes features like antivirus, firewall, and device encryption.
- **Authentication Systems**
  - Employing robust authentication mechanisms, including multi-factor authentication (MFA), to verify the identity of users and devices trying to access the system.
- **Vulnerability Management**
  - Regularly scanning and assessing systems for vulnerabilities, and applying patches and updates to address potential security weaknesses. This helps prevent exploitation by attackers.

Key Elements in Second Line of Defense

- **Incident Response Systems**
  - Establishing processes and technologies to quickly detect and respond to security incidents. This may involve automated alerts, incident tracking, and coordinated response efforts.
- **Network Segmentation**
  - Dividing the network into segments to limit the potential impact of a security breach. This helps contain incidents and prevents lateral movement of attackers within the network.

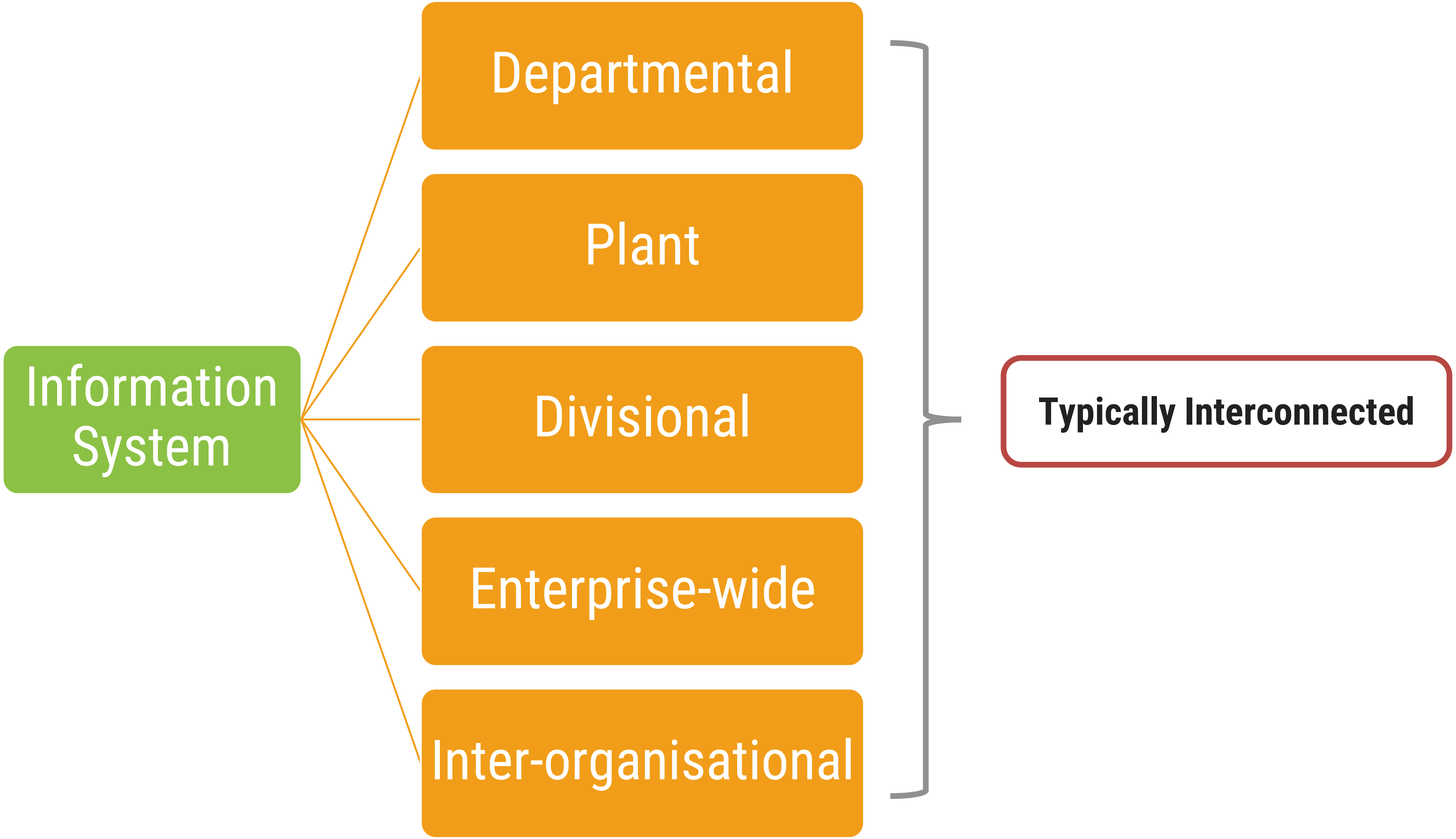
Choice of Information System

- The choice of IT is a **strategic decision making a long-term impact** on the effectiveness of the MIS enterprise.
- The IT affects the **people, processes, and organization** of the system. It is a strategic business decision but not a financial decision taken on the least cost approach.
- Therefore the IT decision is a technical decision where it requires **deciding between the various configuration alternatives made of various hardware-software options.**
- In case of multiple sites of the organization, IT decision must consider the **communication problem and the interface between hardware options** so that the data sharing is optionally feasible.
- The choice of IT is made **based on the availability of the people in the organization to run hardware-software system.**
- IT design is made for **current trends as well as the futuristic needs of the organization**. IT decisions are complex and governed by several factors.

Information System for General Application

- Choosing the right information system for an organization depends on various factors, including the **organization's size, industry, goals, and budget.**
- In the field of Management Information Systems (MIS), organizations often **deploy a variety of information systems to support decision-making, streamline processes, and enhance overall efficiency.**Here are some key information systems commonly used in MIS:
  - Transaction Processing Systems (TPS)
  - Decision Support Systems (DSS)
  - Executive Information Systems (EIS)
  - Business Intelligence Systems (BI)
  - Knowledge Management Systems (KMS)
  - Customer Relationship Management (CRM) Systems
  - Enterprise Resource Planning (ERP) Systems
  - Supply Chain Management (SCM) Systems
  - Collaboration and Communication Systems

Information System for General Application



Information System

Departmental

Plant

Divisional

Enterprise-wide

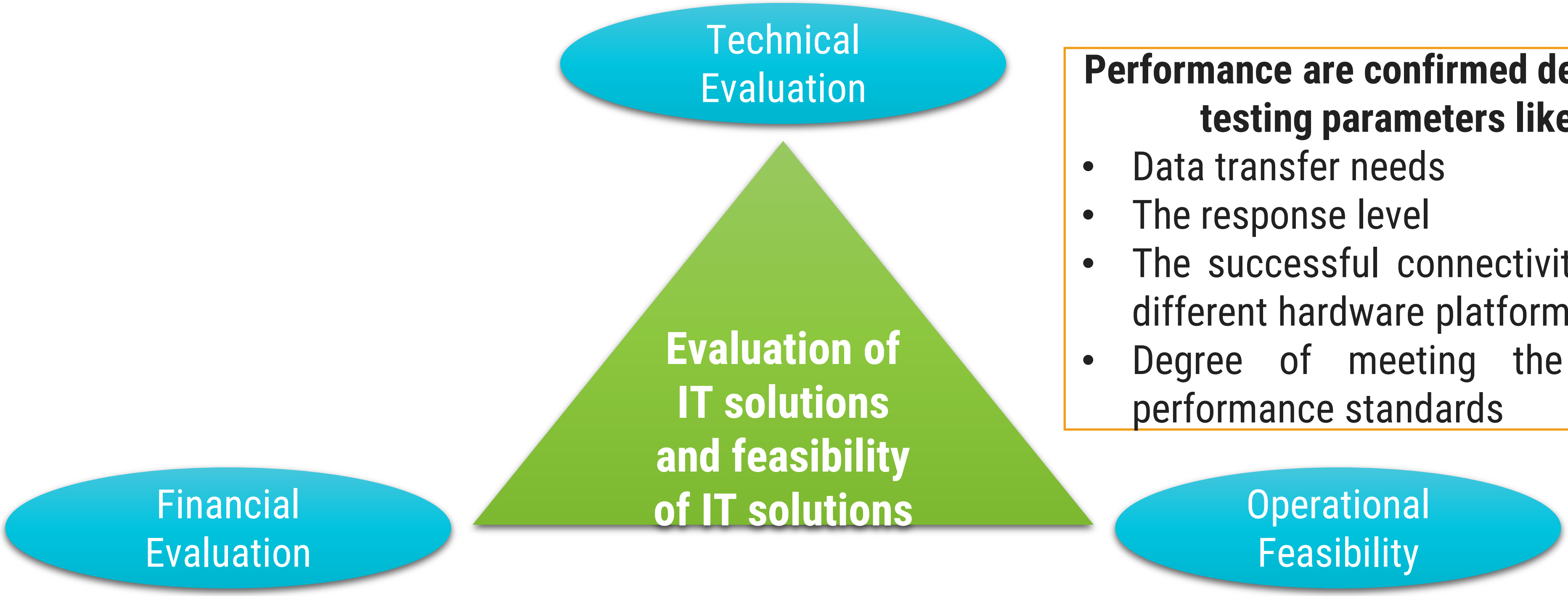
Inter-organisational

Typically Interconnected

Evaluation and Feasibility of IT solutions

- The decision-making enters into the evaluation phase for selection. The different dimensions to be satisfied simultaneously are to have the selection criteria for evaluation as under:
  - Technical Evaluation
  - Operational feasibility
  - Financial Evaluation

Evaluation and Feasibility of IT solutions



Technical Evaluation

Evaluation of IT solutions and feasibility of IT solutions

Financial Evaluation

Operational Feasibility

Performance are confirmed deals with testing parameters like:

- Data transfer needs
- The response level
- The successful connectivity of the different hardware platforms
- Degree of meeting the overall performance standards

Business Investments are evaluated based on:

- Return on investments
- Certain payback periods
- Budget considerations

Considers:

- People related issues
- Whether the systems and the procedures of the organization are complementary and conductive

Strategic Decision

- The information needs of the users in the organization arise from the process or the style by which the management runs the business.
- The quality of management process depends on the culture which affects the decision making process in centralized system; the delegation isn‘t effective and depends on central authority.
- In distributed system it is dependent on different nodal points. There are 3 types of IT decision:
  1. Decision affecting the operational management.
  2. Decision affecting the execution and control of the business.
  3. Strategic decision.

Strategic Decision

- In such cases the IT choice would be the **front end processing connected back to the back office control system.**
- Front end system takes care of **operations managem**ent while the back office takes care of **strategic control and operational planning.**
- Every business has one or more **business-critical applications, serving the other information** needs of the critical strategic decisions.
- The entire process values these applications.
- The organization's IT choice is therefore based on the requirement of these applications serving the critical function.
- Due to the organization's infrastructure and the nature of business IT choice will be distributed at different decision centers.

Business Operations

- There are many organizations where the business operations are **typical and their information needs largely proceed.**
  - Example: Banking organization.
- The decision-making process is **rule based governed by policies and guidelines** in the organization. The IT should specify all the needs in the organization.
  - Example: marketing system- In the marketing of the product, IT processes the data about sales, receipt and other inventory-related information, procurement, actions etc.

Business Operations

- There are certain business organizations, and operations where the **organization takes care of one or two function** and most of the information needs would be satisfied by the hardware software resources.
- If the organization requires **a mix of special platforms** then the IT choice will be based on the integration possibility of different IT platforms satisfying the information needs.
- IT considers the operational feasibility of the system in terms of **data sharing, resource sharing transaction processing**, etc. the number of possibilities emerges unless these factors are properly considered IT choice may go wrong.
- The IT choice therefore is strategic to the performance.

Configuration Design

- **Data type:** Numeric, word, Image, voice and the capable software-hardware to handle these data type.
- **Data volumes:** Floppy drive, hard-disk, CD-ROM with their capacities.
- **Storage capacity:** Based on processing needs of the system.
- **Input/output operation:** It decides the controller and speed of I/O processing.
- **Data sharing:** If data is to be shared then storage capacity will be decided based on the size of the databases.
- **Process speed:** Speed of processing decides CPU, memory processing architect.
- **Query processing:** Decides SQL and 4GL application programs.

Structured Query Language is a domain-specific language used in programming and designed for managing data held in a relational database management system, or for stream processing in a relational data stream management system.

el computer
s envisioned
uages.

Configuration Design

- **Data type:** Numeric, word, Image, voice and the capable software-hardware to handle these data type.
- **Data volumes:** Floppy drive, hard-disk, CD-ROM with their capacities.
- **Storage capacity:** Based on processing needs of the system.
- **Input/output operation:** It decides the controller and speed of I/O processing.
- **Data sharing:** If data is to be shared then storage capacity will be decided based on the size of the databases.
- **Process speed:** Speed of processing decides CPU, memory processing architect.
- **Query processing:** Decides SQL and 4GL application programs.
- **Communication protocol**: If the different platforms need to be connected the TCP/ IP is necessary to be included.

Strategic Information System(SIS)

- Strategic Information Systems (SIS) refer **to the use of information technology (IT) to gain a competitive advantage and achieve organizational objectives**.
- These systems are designed **to support and shape an organization's business strategy.**
- SIS should **align closely with the overall business strategy** of an organization.
- SIS often includes decision support systems. This involves **using data analytics and business intelligence tools to analyze and interpret data** for better decision outcomes.
- They need to be **flexible and adaptive** to changes.
- Organizations must continually **monitor and evaluate the performance** of their strategic information systems.
- In an increasingly globalized business environment, SIS may **need to address international considerations, such as diverse regulatory environments, different cultural norms, and varying customer expectations.**