**Topic 7 Information System**

Most organizations use information systems to operate more effectively, gather information, and accomplish tasks. The term information system refers to a system that uses computers and usually includes communications networks. An information system collects, stores, and processes data to provide useful, accurate, and timely information. Because organizations have different missions and face different problems, they require different kinds of information systems. Examples are online transaction processing system, management information system, decision support system and others.

***The SDLC (planning, analysis, design, implementation, maintenance phases).***

An information system progresses through several phases as it is developed, used, and finally retired. These phases encompass a system development life cycle, usually referred to as the SDLC known as System Development Life Cycle, which provides a general outline of how an information system evolves and delineates the phases of system development.

* The Planning phase for an information system project includes the following activities: assemble the project team, justify the project, choose the development methodology, develop a project schedule, produce a project development plan. The goal of these activities is to create a Project Development Plan.
* The Analysis phase begins after the project team selects a development methodology, draws up the Project Plan, and receives permission to proceed from management. The goal of the analysis phase is to produce a list of requirements for a new or revised information system. Activities for analysis phase are: study the current system, determine the system requirements, and write requirements report.
* In the Design phase the project team must figure out how the new system will fulfil the requirements specified in the System Requirements Report. The project team chooses a solution, selects hardware and software, and designs detailed application specifications.
* During the Implementation phase of the SDLC, the project team supervises the tasks necessary to construct the new information system. The tasks that take place during the implementation phase can include: purchase and install hardware and/ or software, create applications, test applications, finalize documentation, train users, convert data, convert to new system.
* The Maintenance phase is the last and the longest SDLC phase and it lasts until the system is retired. It involves day-to-day operation of the system, making modifications to improve performance, and correcting problems. Three key concepts ensure good quality of maintenance service: reliability, availability, and serviceability. The term quality of service (QOS) refers to the level of performance a computer system provides. Typical maintenance phase activities ensure that the system functions as well as possible.

***System security.***

Threats against information systems are increasing. As with personal computers, common threats to corporate information systems include natural disasters, power outages, equipment failures, human errors, software failures, security breaches, acts of war, and malware. Threats to a corporate information system can affect thousands of people.

Companies can take steps to protect their customers and deal quickly with identity theft incidents, but no computer system can be completely risk-free. Several proactive measures can protect information systems from threats. These measures can be grouped into four deterrents, preventive countermeasures, corrective procedures and detection activities.

* Deterrents reduce the likelihood of deliberate attack. Both physical deterrents, such as limiting access to critical servers, and common deterrents, such as multi-level authentication, password protection, and biometric identification fall under this category.
* Preventive countermeasures shield vulnerabilities to render an attack unsuccessful or reduce its impact. Firewalls that prevent unauthorized access to a system and encryption that makes stolen data indecipherable are examples of preventive countermeasures.
* Corrective procedures reduce the effect of an attack. Data backups, disaster recovery plans, and the availability of redundant hardware devices all are examples of corrective procedures.
* Detection activities recognize attacks and trigger preventive countermeasures or corrective procedures. For example, antivirus software detects viruses entering a system and can be configured to perform corrective procedures such as removing the virus and quarantining infected files.