**INFORMATION SYSTEM BASICS**

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.

A system development project team is assigned to analyze and develop an information system. Other members of an organization might also be asked to participate in various phases of the project.

Justifying a project often involves identifying problems and opportunities within an organization’s current information system. As part of the planning phase, the project team selects one or more methodologies that provide structure for the development effort. The next activity is project scheduling. It begins in the planning phase, but stretches throughout the entire project. Project managers organize the work into tasks and milestones, which can be scheduled and assigned. Project management software is assigned to help in planning and scheduling. It helps managers track and visualize the complex interactions between tasks.

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.

With the escalation of online crime, corporate identity theft has become a major security threat. When a company’s brand is used without authorization, the company has become a victim of identity theft. The Internet makes it easy to steal corporate identities and use them for phishing scams and fake Web sites. It is not difficult for hackers to copy logos and other graphic elements from Web pages of legitimate sites. Creating a fake Web site is also easy.

Several proactive measures can protect information systems from threats. 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. To help minimize risks the hardware and software for most corporate information systems are housed in data centers. A data center is a specialized facility designed to hold and protect computer systems and data. Most data centers limit physical access using password protection and fingerprint identification systems. Motion detectors, automated alarm systems and many other Metrics prevent unauthorized movement through the building.