What is Information Security?

Information Security is simply the process of keeping information secure: protecting its availability, integrity, and privacy.

Information has been valuable since the dawn of mankind: e.g. where to find food, how to build shelter, etc. As access to computer stored data has increased, Information Security has become correspondingly important. In the past, most corporate assets were "hard" or physical: factories, buildings, land, raw materials, etc. Today far more assets are computer-stored information such as customer lists, proprietary formulas, marketing and sales information, and financial data. Some financial assets only exist as bits stored in various computers. Many businesses are solely based on information – the data IS the business.

Information Security is a Process:
Effective Information Security incorporates security products, technologies, policies and procedures. No collection of products alone can solve every Information Security issue faced by an organization. More than just a set of technologies and reliance on proven industry practices is required, although both are important. Products, such as firewalls, intrusion detection systems, and vulnerability scanners alone are not sufficient to provide effective Information Security.

Information Security is a process. An information systems Security Policy is a well-defined and documented set of guidelines that describes how an organization manages, protects its information assets and makes future decisions about its information systems security infrastructure. Security Procedures document precisely how to accomplish a specific task. For example, a Policy may specify that antivirus software is updated on a daily basis, and a Procedure will state exactly how this is to be done – a list of steps.

Security is Everyone's Responsibility:
Although some individuals may have "Security" in their title or may deal directly with security on a daily basis, security is everyone's responsibility. A chain is only as strong as its weakest link. A workplace may have otherwise excellent security, but if a help desk worker readily gives out or resets lost passwords, or employees let others tailgate on their opening secure doors with their keycard, security can be horribly compromised. Despite the robustness of a firewall, if a single user has hardware (e.g. a modem) or software (e.g. some file sharing software) that allows bypassing the firewall, a hacker may gain

access with catastrophic results. There are examples where a single firewall misconfiguration of only a few minutes allowed a hacker to gain entrance with disastrous results. Security is an issue during an application’s entire lifecycle. Applications must be designed to be secure, they must be developed with security issues in mind, and they must be deployed securely. Security cannot be an afterthought and be effective. System analysts, architects, and programmers must all understand the Information Security issues and techniques that are germane to their work.

End user awareness is critical, as hackers often directly target them. Users should be familiar with Security Policies and should know where the most recent copies can be obtained. Users must know what is expected and required of them. Typically this information should be imparted to users initially as part of the new hire process and refreshed as needed.

Information Security involves a Tradeoff between Security and Usability: There is no such thing as a totally secure system – except perhaps one that is entirely unusable by anyone! Corporate Information Security’s goal is to provide an appropriate level of security, based on the value of an organization’s information and its business needs. The more secure a system is, the more inconvenience legitimate users experience in accessing it.

Remember, IT - and Information Security are business support functions:

Unless a companies business is IT, IT is (one of many) business support functions. Many IT professionals lose perspective - we do not!