Definition of security in info. sys

Definition of Security in Information Systems With the advancement of Information technology, more corporations in the world today employ informationsystems to perform basic functions such as input, processing, storage and output of data to convert it into useful information. The core components of such Information systems are People, Hardware, Software, Data and Network. The input process consists of collecting data and transforming it to a form that is suitable for processing. Manipulation of this data gives information (processing). The information thus obtained is either stored for future use (storage), or directed to appropriate user (output).

A very important aspect of such information systems is the ability to protect the data and information obtained from unauthorized access, exploitation, addition, deletion, or modification. This is called as security of information system. Increased interconnectivity amongst various information systems has raised new issues and threats for the security of information systems. However it is based on some core principles. First of these is Confidentiality. It refers to protecting personal privacy, and proprietary information from unauthorized access, and disclosure. If sensitive information such as Card Number No., SSN No., company strategy, transactions data for the company, passwords etc. leaks to unauthorized people, it may lead to large level of misuse by the thief. Second core principle is Integrity which refers to preventing unauthorized information modification (addition, editing, and deletion). The integrity of data and information in an information system may suffer because in many cases like attack of virus/worms, hacking of websites, an employee being able to change sensitive corporate information etc. Another important principle of Information system is to make it reliably and timely accessible to correct users. This aspect of the IS is called

availability. This also includes preventing a website from Denial-of-Service Attacks.

Information system professionals have to protect their corporate IS from various threats. The first kind of threat that can harm the security of IS is hacking, which refers to obsessive or unauthorized use of company computer and network resources. Often employees or outside people make unauthorized use of network, and make fraudulent transactions. This is called as cyber theft. Employees may also use corporate computer and networks for purposes such as e-mail abuses, pornography, and moonlighting. This unauthorized use at work is called time and resource theft. Apart from these, corporate IS may also be attacked by computer viruses or worms. Common sources of viruses include e-mails, file attachments, floppy disks, CDs, or shareware software.

The IS department has to put strict security policy in order to prevent the system from attacks. The first technique that they may use is Encryption, in which sensitive information such as password, messages, and other data can be encoded and decoded using special mathematical algorithms. Encryption methods generally make use of public keys or private keys for each individual. Firewalls which can be used to deter unauthorized access by providing a filter and a safe routing point between the corporate network, and the internet are also a necessity to protect the security of the IS. In order to prevent the D-o-S attacks, IS professionals have to set up defense mechanism at 3 levels. They shall create back up servers at the website. They should continuously monitor traffic and block any abrupt shoot in traffic at the ISP. Enforcement of strict security policies such as scheduled scan for viruses, Trojans etc is necessary at the end-user machines. The IS

department personnel shall install antivirus programs such as MacAfee, or Symantec etc to prevent the IS network from virus attacks. Besides, monitoring of the e-mails to prevent spamming shall be done. Besides, IS department can make use of new technologies such as biometric security, and fault tolerant systems.

Thus, to conclude, Security of IS in an organization is to prevent any unethical practices from employees as well as other potential hackers.