Information Security: A New Managerial Concern

Some 30 years ago, security meant a good lock on the office door! Now, managers and computer users have to be concerned about computer viruses, worms, phishing, spam, intrusion, and identity theft. Security issues and threats in a network environment are varied and can be caused intentionally and unintentionally by insiders and outsiders. They can be categorized as controllable, partially controllable, and uncontrollable. We offer a series of guidelines that should assist key decision-makers and network/computer users to improve the integrity and confidentiality of organizational information, a vital resource complementing labor resources in any organization.

It should be noted that the amount of security budget and protection expenses is often dependent upon the value of the data (i.e., low risk or cost of data replacement would not justify a high cost for security). Some aspects of security measures can be improved and implemented with moderate expenses. Other technical aspects need capital investment in software, hardware, infrastructure, and technical expertise. An organization should carefully consider the security threats and issues and examine those that are particularly related to a specific organization and try to integrate them into its security plan.

To establish a comprehensive security plan, some or all of the following suggestions should be considered:

- Organize a security committee. The committee should include representatives from user groups (including finance, accounting, marketing, manufacturing, and personnel), top management, hardware group, software group, security specialists, and legal department.

- Post the organization's security policies in a visible place and/or in front of every entry port (workstation or PC). The signs should state the organization's policies on security.

- Require all employees to sign an acceptable use policy. This would include appropriate and acceptable network and web access as well as specify punishments as a result of misuse.
Encourage employees’ sensitivity to security problems. This can be done by implementation of a security awareness program. Employees should understand what security risks are and how they can be eliminated or at least minimized.

Revoke terminated employees’ passwords and badges immediately so that a malicious ex-employee cannot be destructive.

Be prepared for computer virus attacks by using the most recent version of antivirus utility programs. Guard against spyware and other intrusive programs by installing a recent version of an anti-spyware program.

Install a firewall that can guard the computer network against many external security threats.

When downloading or copying a file (from the Web or other sources) check it first with antivirus software before copying it to a hard disk or other permanent devices.

Do not allow employees to connect personal computing devices onto the organization’s network without a thorough inspection for viruses and/or other malicious programs.

To minimize legal, organizational and social issues related to the Web and e-mail systems, design, and distribute comprehensive e-mail and Web use policies.

Back-up all of your computer files. Store at least one generation of backups at an off-site facility.

Develop a disaster recovery plan. The plan should outline the actions that will be taken should a disaster strike. The plan should regularly be tested with trial data in order to see the effectiveness of the plan.

Identify all of the vendors and manufacturers of the software and hardware used in the organization. Record the most recent addresses, phone numbers, web sites, and e-mail addresses of these vendors.

Document all the hardware and software in the organization and also document all the changes done to the initial hardware and software. This will help the organization to get back on its feet should a disaster strike.