Chapter 3 - Networking and Group Computing

Security

The need for computer security is changing dramatically as the information technology revolution continues its forward charge. Prior to this IT revolution the primary security was preventing access to a firm's physical office building. Now with high speed modems and portable storage running into the gigabytes security is much more of a threat to protect client's confidences. At the outset, it must be understood that nothing is one hundred percent secure, you can only minimize your exposure. The goal is to minimize your exposure to the risk of security breaches. Also, determine the value of the information that you are seeking to protect. If you control cash or marketable securities, then security is of paramount importance. However, if you are protecting word processing documents that have been backed up, what price do you pay for security? If client confidences are in case management files, then security becomes more important. However, deciding upon reasonable physical security measures, such as double bolted doors, alarms, or 24-hour security guards to guard your paper files, one must also decide when reasonable efforts have been made to secure your computer data system.

As we become more and more dependant on computers and technology, security becomes more important. The security we are concerned about is ensuring that only authorized individuals have access to information, preventing unauthorized alteration, or destruction of data, and ensuring that legitimate users are not denied access to information. To achieve these objectives, we must be concerned about information while it is being transferred from one system to another and the protection of information within a computer system. These measures need to work together with other security measures, including physical security, such as locks on doors, personnel investigations, employee screening, preventing the reproduction of sensitive material, and preventing unauthorized access to on-line data. Other security suggestions are can be found in Chapter 1, *Ethical Issues Involved in Using Technology.*

Considerations:

Office:

- A security plan including policy and procedures should be implemented. This will assist you in avoiding arbitrary claims if you need to take action against an employee for a security breach. Such a plan should be integrated with your overall telecommunications and information system plans.
- Involve your staff in your security efforts.

- Have all staff read, sign and practice computer security policies.
- Check users' access rights on a regular basis to determine the need for staff to access certain areas on the network.
- Passwords - Tell staff you will try to break into passwords. Passwords, keys and other security devices should be secured. Use 8 character or longer passwords that are not found in dictionaries. Frequently change passwords (at least once a month).
- Send staff to security courses.
- Educate staff on insecurity of e-mail.
- Plan on how to handle terminated employees. Terminate their passwords and access codes immediately.
- Ask your staff for suggestions on how to set security policy since they know the weak areas.
- Training your staff on security issues is a must; security will only be as good as the people who implement it.
- Run virus protection software on floppies, servers, and desktops; update your system as new viruses are discovered. The number one way hard drives are infected is via viruses on floppies.
- Write protect your program disks. To write protect have the little switch on the back of a floppy in an open position.

Network:

- Use a firewall to prevent unauthorized access and access to approved users. A firewall serves as a wall between an organization's internal network and a large array of external networks.
- Firewalls are "electronic fences" that keep unauthorized users out of your LAN. Firewalls can range from packet screening router configurations to multiple firewall servers' in-between your LAN and the Internet. The more secure firewalls are, the less convenient it is for authorized users to use the system. Use auditing tools to determine if illegal tampering has occurred. Test your firewall at regular intervals to check for leaks.
- Check who is logging in and out of your network. Lock off certain directories from users.
- Configure system options known to be accessible to security problems.
- Install all vendor security features and upgrades promptly.

Desktop:

- Authentication devices and onetime password generators should be used to gain access to a computer. Biometric devices such as fingerprint readers, facial and iris scanners, hand geometry, signature dynamics, and voice recognition biometric devices should be considered.

However, they can be obtrusive and expensive. A fingerprint reader for a single station can run $100. The best bet may be smart chips embedded in name badges that have to go through a reader to activate the computer.

- Disconnect your system from the WWW when not in use.

Notebook Security:

- Track your notebook with a global positioning system. Absolute (www.absolute.com).
- Tape your business card to the outside and inside of your computer.
- Check your homeowner's or business insurance coverage to see if it is covered.
- Mark your equipment with your social security number using an inscribing device.
- Consider purchasing cable and locks. Kensington (www.zlock.com).
- Encrypt laptop files or have a password to get in.

Encryption:

- Encryption should be a critical cornerstone of your computer security. Data sent, data on laptops, and data sent using an Intranet, Extranet or Internet should be encrypted.
- SSL (Secure sockets layer) is the dominant TCP/IP encryption Web protocol for encrypting general communication between server and browser.
- Point to point tunneling protocol – computers at both ends of the protocol are equipped with identical encryption software and require no special actions by the users.

Web Sites:

- Subscribe to the alert services of the Computer Emergency Response Team Coordination Center (www.cert.org).
- Other security sites - www.sans.org , www.zonelabs.com , and www.securityfocus.com .

- Personal firewall protection - ZoneAlarm (www.zonelabs.com).

Fax Machines:

- Don’t abandon documents that you send from your fax machine if they remain in the tray to be sent.
- An incoming fax may activate your machine’s polling feature, redirecting your fax to whomever just s ent you the fax. Disable your polling feature.

Internet:

- Be aware of rogue Java applets. They can search your computer and upload information back to their site, delete files, and crash your computer.

Remote access:

- Control dial in access by using passwords, callback, and/or electronic ID cards.

Outside vendors:

- Ensure that outside vendors do not breach your security.
- Have them sign security agreements to assist in protecting the attorney client privilege.

Without a doubt, we are accelerating toward an interconnected world using the Internet, Intranets, Extranets and LAN’s. As we transition into this interconnectivity, we must always be security vigilant.