

Secure Your Computer Data

By

Michael R. Arkfeld

Security of computer data is becoming one of the most widely discussed topics in the information age. It is wonderful that the information age has brought the capability of storing, sending and retrieving data anytime and anywhere in the world. However, the dark underside to computing technology is ensuring that your data in networks, desktops and laptops are secured from theft, tampering or outright destruction.

Ethical issues requiring new standards of care are constantly arising as a result of the technology security issues. Losing client data or allowing client confidences to be accessible by unauthorized individuals are a few of the ethical issues that must be addressed. Many office computer disasters and possible ethical violations can be avoided if certain precautions are taken.

At the outset it must be understood that nothing is one hundred percent secure, you can only minimize your exposure. So 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 then what price do you pay for security? If client confidences are in case management files then security becomes more important. In addition to 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.

Theft, computer viruses or hard drive failure can cause security breaches of data. A security plan including policy and procedures should be implemented. This will also 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. The following is a checklist list of the increased scrutiny the legal profession will be expected to address as the technology revolution continues.

- Encrypt laptop files or have a password to get in;
- Tell staff you will try to break their passwords;
- Passwords, keys and other security devices should be secured;
- 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 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;
- Install firewalls on your servers;
- Check who is logging in and out of your network;
- Use 8 character or longer passwords that are not found in dictionaries
- Frequently change passwords (at least once a month);
- Use virus software to scan your;
- Backup your system on a regular basis;

- Run virus protection software on incoming data and electronic information, floppies, servers and desktops and update your system as new viruses are discovered. The number one way hard drives are infected is viruses on floppies;
- Be aware of rogue Java applets – They can search your computer and upload information back to their site, delete files, crash your browser;
- Write protect your program disks. To write protect have the little switch on the back of a floppy in an open position;
- Control dial in access by using passwords, callback and/or electronic ID cards;
- Lock off certain directories from users;
- Install all vendor security features and upgrades promptly;
- Configure system options known to be accessible to security problems;
- Ensure that outside vendors do not breach your security;
- Have all staff read, sign and practice computer security policies; and
- Check users access rights on a regular basis to determine the need for staff to access certain areas on the network.
- Back up your system and have a disaster recovery plan;
- Have two or more people familiar with your computer system, preferably one being an outside consultant;
- Select an outside consultant who maintains confidences;
- Surge protectors and temporary power suppliers should be installed and checked on a routine basis;
- Decide who gets access to information and provide consequences for unauthorized access or attempt to access;
- Preclude access to key areas of the computer operating system;
- Keep kids and others away from your computer at home or at work
- Determine if you have a year 2000 crisis– law firms may have problems with their own computers – visit the www.year2000.com Internet site;
- In word processors there is a feature called UNDO that enables a user to undo the last command. For example if you send an electronic note as part of draft contract to your client and your client read and then deleted the note it can still be retrieved. The other party would just have to UNDO the last command and they could see the note to your client in the electronic contract. Some word processors allow you to UNDO up to 300 of your last changes. Be sure and remove the UNDO feature from the document before it is sent on to the opposing party; and
- Do not send old diskettes to opposing counsel, files can be easily undeleted?
- Can a hacker get into my system? Even if you are not on the Internet, can he call up our office's computer and see sensitive information? What security measures have I put in place?
- Conversations on cellular phones can be intercepted; Cellular phones pose significant risks as to the confidentiality of attorney client communications.
- 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. Test your firewall at regular intervals to check for leaks.

With the proper diligence the transition to the electronic age will pose fewer risks. Ensure your client confidences by practicing safe security.

