



# TECH MOMENTS

## PREVENTIVE PLANNING

### Where Did That Data Go?

Using computers to assist the practice of law can yield great benefits but it requires vigilance in protecting the data you accumulate.

- Create a regular backup of your data and programs on removable media - tape, optical disk, CD-ROM - and keep the backup media somewhere other than your office.
- Use the built-in abilities in your computer to automate data backup, purchase a second hard drive, and synchronize the data from your main hard drive to the second so that, if your main hard drive fails, you have redundant storage for your data.

### Secure the Perimeter

Technology threats are often envisioned as hackers creeping down your wires to steal your data. There are many other, more mundane holes in your perimeter.

- When you have a consultant, temporary, or other employee accessing law firm data or equipment, make sure they have signed a confidentiality agreement and some agreement as to what is an acceptable use of your computer systems.
- Lock server computers in rooms without windows. They should be physically unavailable, so that an unauthorized person cannot remove your data and system files by picking up your computer and walking away.
- Make sure that every computer is running current anti-virus software, and that staff or other attorneys cannot disable the software. A single machine that catches a virus can damage other machines on a network even if it does not infect them.

### Anticipate Business Interruptions

You can call it disaster planning, business continuity, business interruption, but when the power goes out, or you lose your Internet connection or your hard drive dies, you need to have thought out what your next step will be.

- Write down the possible business interruptions - electrical outage, telecommunications outage, etc. - rather than the cause - tornado, flood, aliens - and determine what alternatives you have available. Second Internet connection? Backup generator? Be creative in identifying, or acquiring, alternatives.
- Develop a plan that provides the steps you and your staff should follow when an interruption takes place and practice the plan to ensure that everyone knows what to do and the plan works as you expect it to.

### Fight Fire with Firewalls

Every computer in your law practice that connects to the Internet - either directly via modem or indirectly through a network connection - should have a software firewall installed. This will provide you a defense against possible probing from external threats as well as a line of defense against threats that occur inside your network.