



HOW TO BACK UP YOUR COMPUTER

Disasters happen to someone else somewhere else.

Too bad this isn't true.

Despite being trained – if not genetically hardwired – to anticipate the worst, many lawyers fail to have an adequate backup and recovery system to protect all the important information entrusted to their computers. The information stored on your computer is truly the lifeline of your practice. Safeguarding this information is critical to your practice's survival and an ethical obligation you owe to your clients.

Look around you. If your computer crashed or was ruined in a disaster, how much would the downtime cost you? Even a relatively minor calamity can wreak devastation on your law practice. Just consider the prospect of recreating all your documents, forms, client billing, time records, calendar entries, contacts, and e-mails. Scary, isn't it? If you aren't safeguarding your data on a regular basis, keep reading so you can learn how to get a system in place. Even if you have the support of an Information Technology (IT) department for your law office, keep reading so that you understand what they are doing and can apply it to your home computer.

DATA BACKUP OR FULL-SYSTEM BACKUP?

The term "data backup" refers to backing up or making a duplicate copy of selected information stored on your computer. The term "full-system backup" re-

fers to backing up or making a duplicate copy of the complete computer system – operating system, software application programs, program customizations, folders, and files – not just the data.

The full-system backup is the better choice. Why is a full-system backup so important? Imagine that your computer hard drive has crashed. Everything is gone. Luckily, yesterday you took the time to back up your data by using a computer CD creator program or CD burner program and copied all the important files onto a number of CD-R or CD-RW disks. However, before you can access the information stored on the disks, you must first reinstall Windows and all your software programs, plus all the program updates and security patches. Only then can your computer read the data you saved onto the CD-R or CD-RW backup disks.

If you need further convincing, click the Start button on the lower left of your computer screen, go to All Programs, and look at all the programs you have on your computer. If the prospect of reloading all those programs seems daunting – as it should – consider buying a full-system backup and recovery program for your office.

A full-system backup and recovery software program is inexpensive and easy to purchase. (See Resources at the end of this article.) It will prove its worth in gold, or at least in many, many billable hours. Without it, you would need to manually copy all the data onto CDs – a laborious task that you would likely put off in favor of the daily work of your busy law practice.

DISCLAIMER

THIS NEWSLETTER INCLUDES CLAIM PREVENTION TECHNIQUES THAT ARE DESIGNED TO MINIMIZE THE LIKELIHOOD OF BEING SUED FOR LEGAL MALPRACTICE. THE MATERIAL PRESENTED DOES NOT ESTABLISH, REPORT, OR CREATE THE STANDARD OF CARE FOR ATTORNEYS. THE ARTICLES DO NOT REPRESENT A COMPLETE ANALYSIS OF THE TOPICS PRESENTED, AND READERS SHOULD CONDUCT THEIR OWN APPROPRIATE LEGAL RESEARCH.

CHOOSING A BACKUP AND RECOVERY SYSTEM

A good backup and recovery system has three elements: (1) automatic backup software; (2) a reliable storage device that is kept offsite; and (3) someone who can be trusted to ensure that the system is working. A good backup and recovery system will let you sleep easier knowing that your valuable information is protected.

1. Make It Automatic. The key to the software is that it must work well for the user. Otherwise, the user won't use it. Automatic backup software is the safest choice because you don't have to fit backing up into your day. Instead of an annoying pop-up window asking if you want to back up now or later, it just quickly and quietly does the backup automatically. It doesn't allow you to elbow it aside when you're rushed and taking the short view of your priority list.

The automatic software program you choose should be easy to set up. Typically, once you install the program, an interactive setup allows you to specify what you want backed up, when, and how often. Select a program that has a restore feature so that any archived information can be restored to your computer.

2. Storage Devices. Once you have backed up all the data and programs on your hard drive, you will need to find a place to store the data until you back up again. Dedicating an external hard drive to the backup process is far superior to downloading the backup files onto numerous CDs. An external removable hard drive that plugs into your USB port is a simple storage device. A second removable hard disk drive or other external storage device is an affordable convenience; it will allow you to make a duplicate backup to be stored offsite, with the original locked in your law office's fireproof safe or file cabinet. Consider getting at least a 40 GB or larger external hard drive.

Another storage option is the Iomega Rev, a combination of hard drive and special disks. Useful for PCs or Macs, it is a greatly improved combination of the Iomega Zip Drive and the Iomega Removable Hard Disk Drive. It claims to provide fast and easy backup, disaster recovery, and data transport solutions for a single PC. Other features include password protection, encryption, and removable disks, making it more secure and flexible than an external hard disk drive. The sealed disks are more durable

and have higher capacity than CDs or DVDs. For more information, visit www.iomega.com.

Especially in areas prone to natural disasters, the safest storage of backup information is offsite, preferably in another geographic location. The importance of this topic was recently underscored by the devastation delivered by Hurricanes Katrina and Rita. Using Internet-based backup services is one possible solution, although still controversial. See the sidebar to this article, "Application Service Providers for Online Data Storage."

3. System Backup Policies and Procedures. If you choose a full-system backup software program, your computer backup and recovery system policy is simple because you can set the frequency of the backup. How often should you perform backups? The frequency should be dictated by your comfort level with risking any data created or received since your last backup. Most technology advisors recommend that you back up your new file information once daily, back up your full system once weekly, ship backups out of the geographic area semi-weekly (if living in a disaster-prone area), and do periodic restores semi-weekly or monthly.

Your policy should also designate the person who is responsible for performing periodic test restores to be sure the program is working. Part of ensuring that the system is working is to periodically check to see whether you can restore a file and then compare it carefully with the file you backed up. The restored information should be identical to the backed-up information. The time to check is before you need the information. A recovered file that is unreadable because it is corrupt is not a surprise you want in the eleventh hour of any case.

SELECTING YOUR BACKUP SOFTWARE

When you compare backup software products, look for one that allows you to: (1) recover entire operating systems and/or individual files; (2) schedule backups to occur automatically; (3) customize the timing of backups based on the occurrence of events such as billing; (4) back up and restore quickly; and (5) test the restoration process.

If you need assistance with these or other practice management questions, call the PLF at 503-639-6911 or 1-800-452-1639.

Sheila M. Blackford
PLF Practice Management Advisor