

Covering Your Assets

One day, data backup will save your law practice.

By Ross L. Kodner

While data backup might not be the most thrilling technology topic, lawyers should spend more time thinking about backup systems to protect their increasingly electronic-based, irreplaceable client and firm data. It seems inevitable that there will be a successful legal malpractice suit brought at some point in the future by an angry client when a lawyer fails to protect work product against virus attacks or a catastrophic hardware failure.

It's shocking how many lawyers and firms don't have adequate data backup systems and procedures in place. My own informal survey of continuing legal education audiences show as much as 75 percent of lawyers can't honestly say they could, without a doubt, restore their computer programs and data from a backup made the night before. That truly is frightening.

It's inevitable that at some point the hard drives in your office PCs will fail. The questions to ask are: 1) Will your software survive? 2) Will your critical, irreplaceable client data survive? 3) Will your critical firm systems, such as your billing, accounting and calendaring systems, survive?

The process of backing up your system simply means making a copy of the contents of the hard drives onto some other storage medium. That way, if there is failure of any hard drive, you can restore or rebuild your programs and your data by copying the information you previously copied onto a new or repaired hard drive.

While it seems pretty simple, why do many law firms find the process of implementing and executing backup systems so torturous? It can be a tedious process. Normally, backup involves copying information stored on your PCs' hard drives to some other type of media, such as other hard drives, tape drives, write CDs or DVDs, or specialized data backup Web sites.

Backup Basics

There are some basic rules about data backup every lawyer and law office staff member should follow. Don't back up for the sake of backing up. Back up only so you can restore when necessary. If you do anything in your backup process that could affect your ability to quickly restore your system, stop it now. Other basic rules to follow are:

- Never trust your backup system. Periodically perform a mini test restore to confirm the backup system is fully capable of bringing back your entire system's contents. If you believe your backup software when it tells you it backed up successfully the night before, one time out of 1,000 it will lie.
- Alternate between at least five backup tapes or drives (labeling tapes "Monday" through "Friday" is an easy approach, but more always is better). Alternate among the tapes, and don't rely on a single tape or cartridge over several days. Many firms use 10 tapes or drives, plus 12 monthly tapes or drives used the last day of each month and then archived permanently.
- Store your most recent backup tape or drive physically out of your

office building to protect against fire, theft, vandalism or some other disaster.

- Retire backup tapes after one to two years of use and replace them. Tape stretches over time and multiple uses. It becomes less effective as a result of normal wear and tear. Hard drives used for backup should last longer (three to four years depending on how many are in the alternating cycle). Be sure to erase these discarded tapes because they contain confidential client and firm data.
- Train at least two people in your office how to perform backups, as well as how to conduct a regular test restore operation. Never trust the process to just one person. Have a procedure in which each staffer with backup responsibility checks and confirms the work of the other.
- Don't rely on a single backup method. Employ some type of secondary backup protection.

Back up What?

The only way to truly protect your systems' information is to back up everything on your key hard drives every day. This includes software with the myriad of settings, configuration changes, tweaks, customization, special macros and so forth. It also means your data, including billing and accounting information, calendars, case management information and your documents.

To perform a full back up of your system, you need a backup system with enough capacity to store all the information located on the hard drives you are backing up.

If you have a 120GB hard drive, your backup system should be capable of storing at least 120GB onto a single piece of backup media without using the compression capabilities many vendors tout. You also need data backup software that automatically can perform an unattended backup session, such as in the middle of the night when staff members are not busy working on the firm's system.

An undesirable but commonly used backup approach is an incremental backup, which only backs up files that have been changed since the previous backup. This tends to make for pretty short daily backups. This sounds like a good thing, but restoring from a collection of disks or tapes containing incremental backup sessions can be a nightmare of assembling bits and pieces of a system scattered across multiple media.

Some people think it's OK to back up firm data on a CD, but not back up their programs because they have them all on CD. It's not. Think about all the settings and configuration tweaks in your programs. These need to be backed up. There is no way you will remember all the settings you have made in every application, or the irreplaceable macros in Microsoft Word and Corel WordPerfect, not to mention your Bookmarks and Favorites, as well as the configuration settings and changes in your case management, billing and accounting systems.

Also, layers and layers of patches and updates would have to be reinstalled after you install the CDs. You would have to rebuild Windows itself, patch and update it, and get all the drivers you need. If you can't find your software CDs, you will have to buy these programs again. Most firms don't have the infinite budget and endless time it would take to restore all of this.

It's possible to buy a reliable, working, automated system that can do full backups every day for as little as \$500. It amazes me to see the tortured ways people try to save a little money, making up for it later in scads of lost otherwise billable time.

Tape Backup

Backing up to a tape is an approach that has been used since the early days of legal computing. Today, backing up to tape still is a proven, tested approach that can be cost effective. There are a number of classes of tape backup devices available.

Travan. These are lower capacity drives available from a number of major manufacturers. The highest capacity tapes are referred to as TR-5 and have a maximum capacity of only 20GB per tape, with compression activated (effectively, these are 10GB cartridges).

Advantages: Inexpensive.

Disadvantages: Capacity is too small to be useful today. Travan class tape units are notoriously unreliable, frequently failing to back up information or restore it. These tapes also are prone to physical failure.

Recommendation: Run the other way and never rely on a Travan-class backup unit.

DAT. This used to stand for "Digital Audio Tape," but now is just referred to as DAT. The tapes are called Digital Data Storage. Capacity is up to 36GB per tape, uncompressed with the latest DAT72 standard (up to 72GB compressed). These tapes are reliable, inexpensive and have relatively rapid data transfer times.

Advantages: Inexpensive drive pricing (starting at about \$500) for the DAT72 drives from major vendors such as Hewlett-Packard (www.hp.com). Inexpensive tape cartridges (starting at about \$15 per tape). Proven reliability. Relatively quick transfer rates between 3MB and 6MB per second.

Disadvantages: Relatively low capacity per tape. Larger-scale backup might require manual intervention to change tapes mid-process. Transfer rate too slow for larger capacities.

Recommendation: Perfectly acceptable as a lower-cost, primary backup method for small firms with less than 36GB of server information to back up.

VXA-2. An intermediate tape system that bridges the gap between DAT and Linear Tape Open Ultrium drives is VXA offered by Exabyte. VXA-2 offers up to 80GB uncompressed per tape. The emerging VXA-3 standard offers capacities up to 160GB uncompressed per tape. The combination of ruggedness and relatively low price has created a significant market for the VXA-class devices.

Advantages: Moderate drive pricing (starting at about \$750) for the VXA-2 drives. Inexpensive tape cartridges. Proven reliability. Relatively quick transfer rate of about 12MB per second.

Disadvantages: VXA-2 tapes have relatively slow transfer rates compared to the faster Digital Linear Tape-class LTO Ultrium drives.

Recommendation: Perfectly acceptable as a lower-cost primary backup method for small firms with less than 80GB to 160GB of server information to backup.

LTO or LTO Ultrium. Higher capacity drives in the DLT family descended from the UNIX minicomputer world, LTO drives are rugged, robust, fast and expensive. The LTO Ultrium-class tape drives provide data storage capacity of up to 400GB (uncompressed) and a maximum transfer rate of 80MB to 160MB per second. Prices start at about \$1,800 for the 100/200GB models and can surpass \$2,500 for the highest capacity 400/800GB models.

Advantages: Fastest tape backup method. Proven reliability. Quick transfer rates between 80MB and 160MB per second on the LTO Ultrium series make backing up large hard drives practical in an automated scenario. Very rugged backup tapes.

Disadvantages: Most expensive backup media in terms of both drive cost and tape cost (the latter starting at about \$45 each).

Recommendation: Solid approach. Bar none, the best approach in a tape-based backup system, albeit a bit costly.

There is a hybrid approach in the tape backup arena worth mentioning. Certance (www.certance.com) produces a series of hybrid devices with its CP 3100 series. These devices combine a tape backup unit and a hard drive in a single chassis.

The system initially backs up onto the faster internal hard drive (160GB or 320GB capacity, and sustained data transfer rates of up to 79GB per hour). Then, the system backs up the information to an internal DAT72 tape system for off-site storage. The idea is that the performance drain on a network is less than the traditional tape method because the initial process of copying first to a hard drive is significantly faster. It's an interesting concept. Prices start at about \$1,200.

There are a few tape backup tips to keep in mind. Always buy a cleaning tape and run it monthly. Replace the cleaning tape after 12 uses. This maximizes backup and restores the read and write reliability. Also, consider buying a spare tape drive in case you need to restore three years down the road and your tape drive, attached to the network server, melts in the fire that burned down your office. If your drive no longer is manufactured, it could pose problems restoring your data. If you buy a spare drive and keep it out of your building, you have a spare instantly available.

Hard Drive Backup

Hard drive backup is an approach that is gaining popularity in part because of the striking drop in hard drive costs and in part because of the inherent speed advantage. Hard drives in capacities exceeding 1TB are becoming affordable. With fast Serial ATA interface drives of 250GB in capacity regularly below \$150 per drive, and with fast FireWire and universal serial bus 2 interfaces for external models, this is becoming a popular backup method.

Most data backup software systems support backing up to hard drives, in addition to tape and other media types. As such, it has become entirely practical for the small firm to acquire a batch of five or more external USB2 or FireWire-connected portable hard drives and treat them the

same as if they were tape cartridges for alternating full nightly system backups. Portable drives, such as those packaged in smaller chassis similar to those produced by Iomega, are light enough for off-site transport. Be sure to use a padded carrying case to protect the drives. Cases designed to hold portable DVD players, such as the Targus DVD001 (www.targus.com) or Pelican's 1150 model (www.pelican.com/cases/cases.html) are ideal. There are four approaches in hard drive-based backup.

External portable hard drives. You can get an external portable hard drive with 80GB to 1.6TB in capacity, with either USB2 or FireWire 400/800 connections. In early 2005, hard drives were available in the 250GB range, starting at about \$160 each. Look for lighter and smaller chassis units for easier off-site transportability. Most drive mechanisms are made by either Maxtor, Seagate or Western Digital. Other capable drives are produced by Hitachi, Fujitsu or Samsung.

The same rules for tape backup apply to multiple media backup: three to five drives at a minimum, and more is better for an alternating backup approach. Check out "The Three R's of Data Protection" (www.dlftape.com/ThreeRs) for a good example of an alternating backup approach.

Internal removable hard drives. In this approach, there is a removable hard drive bay mounted in the network file server internally. A good example would be the removable Data Express series of backup drive systems from StorCase Technology (www.storcase.com/dataexpress_bu/backup_overview.asp). Individual hard drives are mounted in removable carriers. These slide into the mounting bay in the file server system. The connection system is either Parallel ATA or the faster Serial ATA. Internal removable hard drives also are available under the Kingston Technology brand. A set of a single receiver and five carriers ready to have hard drives mounted in each carrier would start at about \$460, plus the price of Serial ATA hard drives up to 400GB in capacity.

This approach offers higher potential data transfer speeds than external USB2 or FireWire 400/800 drives through the Serial ATA interface method, up to a theoretical 150MB per second for Serial ATA and up to 300MB per second for the newer, faster Serial ATA II class drives. Portable drives should be stored off-site nightly and carried in a well-padded carrying case.

CDs and DVDs. The quick answer is "no." Writable CDs and DVDs are not suitable for system backups. CDs only hold about 680MB of data and DVDs hold up to about 4.7GB (or about 3.5 times that with dual-layer DVDs). However, there isn't enough capacity on the media to perform automated full system backups. Also, when backing up to a CD, you have to do it manually by changing the media to a new CD or DVD when prompted. Most firms don't have that kind of time. CD and DVD are better for smaller-scale spot backups or secondary backup approaches.

Network Attached Storage. This class of network hard drive systems has been around for years. These devices can be attached to a Windows or Novell network, and configure and map themselves as an available network drive letter. The original product in this space was called the Snap Server. Today, there are a broad range of such devices. Most portable drive manufacturers offer some sort of networked version of their hard drives.

Companies such as Seagate, Buffalo, Western Digital, Maxtor and Ximeta all offer simplistic NAS devices. But for network-smart systems that recognize and connect to Windows Server and Novell Netware systems, a step up the ladder is warranted. Snap Appliance, the original makers of Snap Servers, has become a division of Adaptec (www.adaptec.com), with models ranging in capacity from 80GB to 30TB. These devices can make an excellent secondary backup system, but not a primary backup system because they are too bulky to take off-site on a regular basis.

With GuardianOS and BakBone NetVault software, these systems are ready to serve as capable and powerful in-house backup systems (www.snapappliance.com). For smaller firms, pricing for the Snap Server 1100 model with 160GB of capacity costs about \$475, while the 500GB Snap Server 2200 model costs about \$1,200.

Get Covered

Backup isn't exciting to think about, much less actually have to do. However, it's the single technology that can one day save your law practice as a business.

Remember the basics: full backup, no shortcuts, regular test restores, alternate the media, replace the media periodically, never rely on just one backup method, think about downtime reduction and have multiple people responsible.

Part 2 of this backup series, which will be published in the October/November 2005 issue, will focus on Internet backups and alternative backup solutions that have become increasingly popular in recent years.

Ross L. Kodner, an attorney, is founder and senior consultant for 20-year-old MicroLaw Inc., helping law firms and legal departments understand, select and better use technology in the workflow of their practices. He can be reached at rkodner@microlaw.com and (414) 540-9433.
