

TECHNOLOGY REPORT



Backing up is a saving grace

By Sheldon Penner

Where would you be if you had arrived at work this morning and all the data in your computer was gone? Would you have a backup of all the documents you were working on the day before? How long would it take to be up and running again? If these questions leave a sour feeling in your tummy, you might not have an adequate data backup plan in place.

For any business, an ongoing system for backing-up computer data should be a key ingredient. For a trial lawyer firm, with confidentiality issues and irreplaceable memos, the importance is intensified. To help you develop your backup plan – or review the plan you already have in place – five methods for archiving and recovering your data are presented below. Every office has different needs and a system that works well for one firm may not be applicable for others. The main lesson here is *any* backup plan is better than none.

Writing to a CD

Backing up to CD is a very popular method and for the most part is relatively simple. All it takes is blank CDs, a CD writer or burner in your computer and a CD burner program. Blank CDs, purchased in bulk, now cost less than 50 cents each. CD writers have dropped in

price to less than \$100 and many new computers come with the writer already installed. The burner software is usually included with the hardware.

You simply place a blank CD in the writer, use the burner software to select the files you want to save and burn a new CD. Presto, you have an archive of the data on your hard drive. Burning CDs is a good method if your documents will all fit on one or two discs. A CD generally holds about 640 megabytes of data. For many attorneys, the most important files are Word or WordPerfect documents that take up little room. It could be possible for a solo practitioner to backup five years of archives on one CD.

An important part of your backup plan is the storage site. If all of your backup CDs are in your office and your office is burglarized, your backups could disappear with your computer. You want to move your archived data to a safe site away from your office. Taking newly archived data home every night is a good solution.

Using CD media does have its disadvantages. The sheer number of CDs can quickly become overwhelming and if not properly labeled utterly useless when it comes to restoring old files from previous days, weeks or months. You should label each CD with the date and a description of what's on the CD. Establish a storage system so you always know how

to find your most recently archived CDs and so you can quickly place your fingers on data from a particular time, say one year ago.

If confidentiality is an issue CDs are not a good choice since it is harder to password protect the backup. If the backup was placed in any CD reader the data could be accessed and read causing a potential liability risk.



Portable hard drives like these from CRU DataPort are an affordable backup option.

One solution to ending up with a large number of CDs is to keep saving to the same CD, and then, perhaps once a week, putting that CD in storage and starting over with a brand new one. Saving to the same CD over and over again is called CDRW or CD write/rewrite. To do this you must have a CDRW burner and blank CDs formatted for CDRW. That is not a big problem these days as most CD burners contain the “rewrite” function.

There are a couple of considerations to saving to the same CD more than once. First, you could lose a document from earlier in the week by saving over it. Second, to ensure the integrity of your archived data, it is a good idea to never re-save to the same CD more than a few

times.

The DVD dilemma

DVD media is another form of backup that closely represents the use of CDs. The big difference is that a DVD can hold 4.8 gigabytes of data or about seven times more data than a single CD. If you use a lot of photos in your practice or create multi-media presentations – both of which can take up large amounts of storage space – a backup system using DVDs could be right for you.

A writable DVD drive can run you about \$150-\$350 and blank DVDs generally cost one to two dollars each.

There is one important drawback to DVD archiving. The recordable DVD manufacturers are still unsettled on a single, universal format. As a result we have two main types: the “plus” format and the “minus” format. Most DVD burners that come in new computers are combo burners so you can choose which format to use. However, because the format is not standardized, you are advised to engage in a trial and error process to determine which format works the best in your computer.

Someday, a single DVD format will emerge. To protect yourself against that eventuality, hang on to the DVD software and hardware you are using to make sure you will always be able to recover your archives. You don't want to be left high and dry if your chosen format isn't covered by manufacturers in the future.

Tape for the traditionalist

A backup system that employs tape has been the accepted means for offices large and small for several years. The tape media has become smaller in physical size, larger in a capacity and longer-lasting. In the past several months, the falling cost and increasing reliability of removable and portable hard drives has caused many offices to re-evaluate and

replace their tape drive backups. Still, tape can be a solid and reliable medium for data archiving.

You need to install a tape drive on your computer or server. The cost of a tape drive ranges from \$300 to thousands of dollars. We suggest 22 tapes for a thorough backup rotation – one tape per business day. Tapes are made from a variety of material and have a very wide range in cost similar to the drives. You will also need backup software that will work with your tape drive – basic software is usually supplied with the equipment. But if you have a server, to really take advantage on the tape system, you will need to purchase additional software that could cost several hundred dollars.

The GFS (grandfather, father, son) system is a commonly accepted tape rotation strategy. GFS simplifies tape handling by organizing rotation into daily (son), weekly (father), and monthly (grandfather) backup tapes.

The GFS tape rotation strategy is based on a five day schedule (Monday

through Friday), in which you create at least one full backup each week. The rest of that week's backups can be full or differential. (A differential backup saves only the files that changed since the last full backup.)

Regardless of the number of full backups you create during the week, the last full backup of the week is considered the weekly backup. You can reuse the daily and weekly backup tapes or take them offsite for permanent storage.

With tape backup you will want to research and commit to a solid plan for rotation and storage. For example, at the end of each week you could take a week's worth of tapes home to store off-site. The following Monday, bring in the previous week's tapes and place them back in the rotation.

Things to consider with tape. The average tape can only be used five to 30 times before it's chance of failure increases. Tapes also have a limited shelf

See Technology p 30

ONE FIRM'S BACKUP

We have used an off-site backup service for over 6 years. You simply install the software, choose the files you want backed up and how often to back them up — from there it's automatic. We back up all our case files and program databases daily. You can backup data from single computers or, as we do, networked computers. Since the backups are online and offsite, there's no worry about tapes or disks. Every week or two I check the backup logs to see that everything's working properly, but that's it. If you do need help, tech support is immediate and personal.

The test of any backup system, however, is how reliably a lost file can be retrieved. Several times we have restored a lost document seamlessly. It takes maybe a minute or two. When our entire server crashed, we were able to reload every document and all databases directly from the service, losing nothing.

*Mary Hallman, Office Manager
Hallman & Dretke, Attorneys at Law
W. Eugene Hallman, OTLA President's Club
Brian C. Dretke, OTLA President's Club*

life unless stored in ideal conditions. If you are using tape, be sure that you know what is the best way to store that particular brand. The time and cost of purchasing new tapes and replacing old ones has to be accounted for in your plan.

The most important thing with tapes is to verify the backups on at least a monthly basis. The best procedure is to check weekly to make sure you can recover and restore data that has been stored on tape. In some systems, a tape drive can appear to be backing up your data, when nothing is happening. Pity the attorney who experiences a hard-drive crash, goes to the tape archive and finds there's nothing there.

Portable hard drives for simplicity

With the price of hard drives dropping almost daily, removable or external hard drives are one of the most cost effective methods of backing up. External hard drives are connected to one's computer by either USB or firewire cables and to the user look just like another drive on the computer. Removable drives are hard drives that have a slot in the case of the computer and slide in and out and are locked in place with a key. These drives usually work faster than an external hard drive and have the feature that they can be completely encrypted for added security.

Portable hard drives are attractive because they hold so much data. A portable hard drive can hold between 40 and 300 gigabytes, the same capacity as your office computer. Since the cost per GB is relatively inexpensive it may be possible to do more complete backups, decreasing your downtime in event of data loss.

A 40 gig portable hard drive will cost approximately \$150. For this system you will also need backup software. A vari-



A M I C U S D A T A
GETTING DATA BACK UP

**YOUR TIME IS MONEY.
DON'T SPEND IT WORRYING ABOUT
YOUR COMPUTERS.**

**Crash Proof Servers
Individualized Data Backup Plans
Easy & Reliable Offsite Storage Systems
Network Configuration & Troubleshooting
End of Life Hard Drive Data Destruction**

**503-516-8618
SHELDON PENNER
INFO@AMICUSDATA.COM
WWW.AMICUSDATA.COM**



Approved Partner
NET INTEGRATION TECHNOLOGIES

ety of backup software packages are available for downloading off the Internet for anywhere from free to \$200 and up. Most of these have free tryout versions so you can try before you buy and offer features such as encryption and virus scanning so your backup is safe.

Backing up to these drives simply involves setting the backup software to run on a daily basis – the middle of the night is a good time – and then swapping the drives on a regular basis. The advantage of hard drive backup is that hard drives these days are made very rugged and can withstand more “rough” handling than other forms of backup media.

It is recommended that one has at least two (more is better) drives that can be rotated regularly. The rotation could be weekly to daily. Drives not being used should be stored offsite. One drive would

be in your office for backup. Then – say, once a week – you switch the drives. At the end of the year one of the drives is removed from the rotation and placed in storage. A new hard drive is then added to the rotation as a replacement. Hard drives can last for many years in storage.

Leave the backup to someone else

The most popular and reliable data backup strategy in today's technology includes an offsite service with an independent third party. Professional offsite services include individual support, local scheduling and processing, data encryption and secret password protection assigned to all data transmissions. The remote data vault contains only encrypted, password protected client data and can only be accessed by the client. Offsite backup service fees for small businesses, (about \$40 per month) generally

include 500-1000 megabytes of compressed data, one to six months online availability to archived data, and periodic media images of retired archival data sent to the customer. With this method, little user intervention is needed after the first install other than checking the logs and adding files as needed.

Summary

Determining what is the best backup may include incorporating more than one of the above methods. One key to backup is to always schedule time for test restores to test your backup. There is nothing worse than having a failure and then finding out that your backup did not work. Another point is to always have a copy of your backup offsite. Keeping your archived data on top of your computer is a danger sign. Any catastrophe that ruins the computer will most likely ruin the backup as well.

Computer data can be a very powerful tool in a trial lawyer's practice. We have all placed our faith in computer technology because the technology has proven to be so effective. However, you should not let yourself be fooled by the seeming reliability of this technology. Bear in mind that computers have a relatively short service life, represent a data system in constant migration and can fail at the most unexpected times. Good backup is good business. A trial lawyer without a reliable and proven backup system might soon be out of business.

Sheldon Penner operates Amicus Data, a computer consultancy that specializes in data backup, harddrive duplication and office networks. You can reach Penner at info@amicusdata.com and you can learn more about Amicus Data at www.amicusdata.com.

*Asbestos
continued from p 27*

tial factor in the later development of mesothelioma, an asbestos-related cancer. If a court followed the *Kowalski* holding, the statute of ultimate repose could be tolled for a household type of exposure. The irony of this claim would be that a premises liability claim would then exist, but for the person who was never likely exposed to asbestos on the premises.

Conclusion

Asbestos injuries, like other toxic torts, have long latency periods. While Oregon's asbestos saving clause allows product liability actions to be brought without regard to Oregon's 10 year statute of ultimate repose, a premises liability claim will likely fall outside of the savings clause. Because the latency period for disease is longer than Oregon's statute of ultimate repose, premises claims for asbestos-related disease will probably fail unless an alternative theory to extend the statute is available.

Possible exceptions to the statute of ultimate repose include the "owner as contractor" theory and CERCLA. As set forth above, both are of doubtful utility.

A plaintiff could bring a claim for intentional infliction of emotional distress based upon asbestos exposure. Such a claim could be brought immediately after exposure and well within Oregon's statute of ultimate repose. The difficulty with such cases meeting the stringent standards for such a claim and the attribution of damages, which would be for emotional distress not asbestos disease.

Until such time as the Oregon Legislature finally appreciates the capriciousness of its present approach to tort limitations and alters the statute of ultimate repose, suits for asbestos related injuries based upon premises liability theories will be very difficult for the majority of

plaintiffs and rarely successful.

¹ If the asbestos workers' compensation claim is denied on the basis of major contributing cause, the worker would likely have a claim pursuant to *Smothers v. Gresham Transfer*, 332 Or 83, 23 P3d 333 (2001).

² *Rich v. Tite-Knot Pine Mill*, 421 P2d 370, 245 Or 185 (1966), *State v. Johnson*, 628 P2d 789, 52 Or App 651 (1981), Restatement 2d Torts § 329 (1965), UCJI 46.03.

³ *Rich v. Tite-Knot Pine Mill* 421 P2d 370, 245 Or 185 (1966), UCJI 46.05.

⁴ *Taylor v. Baker*, 566 P2d 884, 279 Or 139 (1977), *Reed v. Jackson County*, 803 P2d 1194, 105 Or App 24 (1990), rev. denied, 311 Or 261 (1991), Restatement 2d Torts § 332 (1965), UCJI 46.07

⁵ Restatement 2d Torts § 332 (1965).

⁶ *Rich v. Tite-Knot Pine Mill*, 421 P2d 370, 245 Or 185 (1966), *Denton v. L.W. Vail Co., Inc.*, 541 P2d 511, 23 Or App 28 at 32 (1975), *Hansen v. Cohen*, 276 P2d 391, 203 Or 157 (1954), UCJI 46.04

⁷ Restatement 2d Torts § 333 (1965).

⁸ *Blystone v. Kiesel*, 431 P2d 262, 247 Or 528 (1967), *Ragnone v. Portland School District No. 1J*, 633 P2d 1287, 291 Or 617 (1981), UCJI 46.06, UCJI 46.06A.

⁹ *Blystone v. Kiesel*, 431 P2d 262, 247 Or 528 (1967), *Ragnone v. Portland School District No. 1J*, 633 P2d 1287, 291 Or 617 (1981).

¹⁰ *Id.*

¹¹ *Rich v. Tite-Knot Pine Mill*, 421 P2d 370, 245 Or 185 (1966), UCJI 46.08.

¹² *Briggs v. John Yeon Co.*, 122 P2d 444, 168 Or 239 (1942).

¹³ Some courts have also held that the CERCLA tolling statute applies only to CERCLA Superfund sites. *Knox v. ACandS*, 690 FSupp 752, 758 ("in fact, the wording of §9658 and its incorporation of the terms of CERCLA and the CERCLA definition of those terms indicate that the provision was limited to application in the situation where a state cause of action exists in conjunction with a CERCLA cause of action. That not being the case here, the court finds that §9658 is inapplicable and therefore, that it does not serve to pre-empt Indiana's statute of ultimate repose in this case").

Jeffrey S. Mutnick is with the firm Landye Bennett Blumstein LLP. He is a member of the OTLA President's Circle at the President's Club Plus level. His offices are at 1300 SW 5th Ave Ste 3500, Portland OR 97201.