



Data Preservation and Recovery, Part 2

by Cindie Gruetzmacher

Editor's Note: Last month, we covered some of the basics of keeping your computer healthy. You learned about virus protection, data-theft, backup strategies, and types of backups. This month, Cindie discusses when to run a backup, how to develop a plan for media rotation, and how to determine what types of data to backup. She will also look at the restoration process and examine more precautions you should take to avoid any "data doom" should your computer fail.

When to Run a Backup

Performing a backup *every day* will provide the best security. However, running it every other day or even *once a week* may be okay in your situation, especially if you don't input data every day. You also may choose not to backup daily if your backup procedure requires an excessive amount of time swapping media. Just make sure you have hard copies of the work you've done so that recovery (i.e., manual input) will be complete.

If you occasionally backup the entire computer system, then do it again *prior to making major program or hardware changes*. Then if the new program or hardware cripples your system, you

will be able to restore the system to its former state. After making the major changes, if all is well, run another entire system backup to retain the new data. Even better, maintain a backup set of both the before and after, and label each accordingly.

Most companies prefer to run an unattended backup after business hours. The advantage is that all of your selected files should be closed and thus will be backed up. A spreadsheet that is open, for example, will be skipped during the backup process. Make it a policy that everyone logs off the network at the end of the workday for backup purposes as well as security. (Better yet, an NT/2000 Server can be configured to log users off at specified times.)

Media Rotation

You should do, at the very least, a *two-day* media rotation. For example, with tapes as the media of choice, you remove Tape #1 from the drive and insert Tape #2—it's ready for the night's backup. You take Tape #1, which contains the previous night's backup, home with you so that it is off premises in the

event something destroys the data in the server and on Tape #2. A better rotation incorporates five tapes into a *five-day* rotation, always taking the most current one offsite. This gives you a cushion in the event one of the tapes becomes unreadable, or if there was virus damage you didn't notice for a day or two. You can double or triple your tape backups by appending a second or third backup to the same tape, rather than overwriting the existing data. Avoid appending consecutive days on the same tape—append a Monday backup on a Monday tape, etc.

Plan in advance the amount of media needed to store your backups. Multiply the quantity of media required for the job by the number of days you want to include in the rotation. If backing up with your CD Burner uses two CD-R/RWs and you want to do a five-day rotation, then you'll need ten CD-R/RWs. Be sure to label your media so you can easily keep track of which is used on what day. Purchase the re-writeable CDs if you plan to use them more than once.

In addition, you may occasionally want to archive a backup. For instance, you could run a backup prior to closing your accounting software for the year. Set the write-protect feature, then label and store this year-end backup in a safe place, and it will be available if you ever need to recreate that year's data.

Data to Backup

If you have the time and media capacity, you may want to perform a full backup of *everything on the hard drive(s)*. To save time and space, you could intersperse with incrementals or differentials. Or you could run this "full on everything" procedure just once or twice a year.

Performing a full backup of *only data files* will save time and media space compared to backing up the entire system. On subsequent days, you could again run incremental/differential backups or just go ahead and run a full backup every time. Data files are the files you've created including documents, spreadsheets, accounting data, images, drawings, audios, videos, templates, and personal information manager (PIM) data like schedules and extended customer information. Don't forget about Internet browser and email account data like your bookmarks, address book, and saved email. MS Outlook data is stored in the *.pst* file and Netscape's data will be the

entire user folder(s) located in its program directory. You may have to do some digging to find the locations where your data is stored. Use the Windows *Find File* feature to help you first locate your files—click *Start, Find, Files or Folder*. After creating your first "backup job" in the backup program, you should not have to go through the entire selection process again.

Always backup the *registry files*. The backup program may automatically select these files for the computer it's installed on. Confirm it. Be aware that you will need to select the registry files of networked machines. On Windows 95/98 computers, you can find the *system.dat* and *user.dat* registry files in the *windows* folder.

Many people religiously run a backup daily, but they don't bother to look at the backup log. Suddenly the time comes to restore data and, oops, there's nothing on the tape! Confirm that you are getting good backups; in fact, practice doing at least one restore.

More Precautions

In addition to preserving and backing up data, prepare tools that

will assist you in getting into your system in the event it fails to boot. Create a *Startup Disk* (boot disk) for each Windows computer. One way to do this is by using the *Startup Disk* wizard found by clicking *Start, Settings, Control Panel, Add/Remove Programs* icon, *Startup Disk* tab. You should be able to boot your system

There may be as many data preservation and recovery policy variations as there are businesses. That's one of the glories of owning your own business—you can do it your way.

using the Startup Disk, which will enable you to get into DOS, gain access to some system diagnostic utilities, and use your CD drive. Some backup programs come with recovery utilities as well, which you create during or after installation of the software on floppies and possibly other media. For Windows NT and 2000 machines, keep the *ERD* (Emergency Repair Disks) updated. Also, if your hard drive is partitioned, write down the size of the *partitions*, as that can play a big part in the ability to restore your data.

Continued on Page 36

**You've Worked Too Hard To Find Your Customers,
Don't Risk Losing Them With Chemicals
That Only Work Sometimes!**

We Can Solve Your Problems . . .

We've spent 32 years formulating cleaning products specifically for the Pressure Washing Industry. We manufacture the **most effective and highly concentrated** line of cleaning chemicals on the market. This provides you, the distributor, with the opportunity to **secure your customers** for the long haul and **maximize profits** at the same time.

Our expertise and knowledge of the **problems you face every day** is unsurpassed. No one knows more about Pressure Washing than we do. **Use this to your advantage.**

Call **Keystone CLEAN-X**, producers of the original two-step cold water, brushless truck washing system.



Professional Lab Analysis
Expert Custom Formulating
Complete Line of Liquids & Powders
for Industrial Cleaning

Keystone CLEAN-X, Inc.
(800) 784-9370

Protected Distributor
Areas Available

For more information circle 375

Restoration

In less extreme circumstances, data restoration can be fairly simple if the groundwork has been laid properly and kept up to date. If you've backed up the *entire system*, and it was healthy, you should be able to restore it to the repaired or a new hard drive. (Be sure to use the FDISK utility and format the new drive prior to the recovery process. See

Make it a personal goal to implement your company's first or improved data preservation and recovery policy over the next three months. Take action and make it happen.

the manufacturer's instructions.) If there were previously partitions, then the new ones will need to be the same size or larger.

If you've backed up *only data files*, recovery of a fixed disk failure will take longer, as you'll need to first install the operating system, programs, downloads, patches, drivers (such as for video, audio, or network adapters), then finally your data. Reconfiguring your personalized settings will take time, too, as well as bringing it back onboard a network. Keep in mind that even with daily backups, you could still lose up to one full day's work, which will need to be input again.

After restoring the system, it would be a good idea to update your anti-virus software and *run a system scan*, especially if you don't know what caused your problem.

The first data restoration you perform (other than the practice one) will more than likely require recovery of just a few files, usually registry files. Another likely candidate is a database, which can become corrupt just by the nature of what it is, although many times these programs

will include a rebuild utility. But your strategy should include plans for the worst case scenario—total data loss.

Note: When doing the *practice restoration*, send the data you select to restore to a "test" folder, or, create a data file specifically to be backed up and restored. You don't want to risk writing over current files with old data.

Other Options

There may be as many data preservation and recovery policy variations as there

are businesses.

That's one of the glories of owning your own company—you can do it your way.

Knowing that, I should mention there are on-

line data storage services. Using the service requires a software download. The user pays a monthly fee based on the quantity of data stored, anywhere from \$5 to \$50 and up. The service works best if you have a broadband Internet connection. I have not yet crossed paths with anyone who has chosen this method of data storage. Most people hold their data very tightly. To see what Connected has to offer for enterprise data management, check out their website (www.connected.com).

For my own small business, once a week with a floppy, I backup accounting data using the backup utility that's included with the accounting program. I then restore it to a second computer and verify that the data is good. (This functions as my "manually mirrored" partition.) I jot down the backup date on a sticky note, post it on the floppy, then store it in a secure place. This takes less than ten minutes. If my system goes down, I can immediately access my clients' information from the alternate computer if needed. To backup the rest of

my data files, as well as programs and patches I've downloaded, I use a CD Burner. In fact, rather than actually doing a backup, I copy them to two CDs. Now if my system goes down, I won't have to go through the restore process but can access my data files from any computer with a CD drive that's running the necessary programs. Burners take a bit longer—my procedure takes about 35 minutes, and I only do it twice a month.

Another safety net I use is to save a lengthy project I've been working on to a removable disk (floppy or CD) or, at the very least, print out a hard copy. If my system keels over after 12 hours of work, the backup I did the previous day/week won't help me a bit.

Personal Goal

If your data preservation and recovery policy is already in place and you're satisfied with it—Congrats!! If your system is not protected and you've felt the dark cloud of impending data doom hovering over you, then maybe this little overview can help get you on the road to data integrity recovery.

Make it a personal goal to implement your company's first or improved data preservation and recovery policy over the next three months. Take action and make it happen. No matter how small or large, you are a contributing part of this country's gross domestic profit. The loss of your company would impact not only you and your employees, obviously, but the country as well.

Make September 11, 2002, a day not only of mournful remembrance, but one of diligence. With your mind fixed on the worst case scenario, be resolved to persevere—do it as your company's part in the world's war on terrorism.

Cindie Gruetzmacher has been providing IT support for small businesses since 1990. She emphasizes optimizing system resources and user knowledge in an effort to improve overall efficiency. 🖱