

# Verifying, testing your backups is a must



John Deans

I had not heard from this client in almost a year since he was one of those guys that wanted to do the whole IT thing himself, but this time he sounded very concerned. Frantically he told me that he was having trouble restoring files from his backup since his hard drive had just crashed.

Arriving quickly I soon discovered that he had only been copying and pasting the shortcuts on his desktop to an external memory stick and never really backed anything up. He was devastated after I told him all his data was gone and he then realized that I had offered to help him set up a solid backup solution for him the previous year, but he refused.

They say live and learn but lessons like that are hard ones to take. Data loss is a serious consequence of either apathy or lack of experience when setting

up backups properly. These days, data integrity and stability are absolutely critical.

Businesses that have catastrophic data loss can be the death of a company, especially with the economy in the pits already.

Configuring and monitoring data backups are daily chores that I constantly fret over. By far the most important thing I do is make darn sure all data is backed up so it can be restored in case of hardware failure, human error, theft or even fire.

A couple of months ago Jim McIngvale, owner of Gallery Furniture, was able to rebuild and reopen their original huge store on July 4 after a devastating fire. He stated that the only reason he was still in business was due to offsite backups of his computer system.

The first step to take is setting up backups which can be done

in a variety of ways that we have covered in previous articles. Whether you use tape, CDROM/DVD, flash drives, external hard drives, or online backup services, there are other processes you must go through to insure that the solution is solid and actually works both ways.

What good is it to backup data up if you cannot retrieve it in a clean and quick fashion? Decades ago, I stopped doing incremental backups dumps and went only with full backups every night. This was because of a bad experience I had reconstructing a data set from multiple tapes that covered a month's worth of work.

One of those tapes had a physical problem and I had a heck of a time getting the data restored properly due to the missing link. It worked out but it took me days to fix it and introduced me to my first chest pains at the ripe old age of 25.

The important issue here is to test your backups to make sure they are working. This includes

verifying that all the files necessary to run the system and all data are being properly backed up to some sort of reliable media.

Whether you use the native Microsoft Windows backup (NTBackup.EXE) or Backup Exec by Veritas (Symantec), you first should monitor the backup log files to make sure the backup ran the previous night and no files were skipped.

Depending on the database application I have seen files never getting backed up because some process had it locked up preventing certain backup software from making a copy of it.

Eyeballing the backup logs takes discipline but is very important and necessary to be done consistently. Could you imagine what the IT team at Gallery Furniture was thinking when they were watching those flames shoot out of the store that night?

Probably something like, "Please God, tell last night's backup made it to the offsite facility."

Most third-party backup applications can e-mail the log files to you which help the verification process. For my sites that run the vanilla MS Backup procedures, I quickly glance at the .BKF files to verify the date and size which quickly tells me that all the stuff got backed up the previous night.

After you have established this daily backup verification process, there is another step that needs to be performed every few months to check your backup solution is solid. This operation is a restoration test which is done by performing a partial restore of one or more files and directories from the last backup to a temporary target area.

In other words, you need to actually restore some files from the backup tape, hard drive, DVD, flash stick or remote service like DataDepositBox.com, Carbonite.com or Mozy.com.

There is no need to completely restore the whole hard drive or reload the operating system, but at least load back a folder with critical files onto a scratch directory and try opening the file.

Not only will you be verifying the backups are good, the media is accessible and the files are actually there, but you will be familiarizing yourself with

the restore side of the backup application and learn how it all works. Many users of Veritas had never really tried the Restore section of the program and do not understand how complex it can be.

Also with Veritas (Backup Exec), there is an option called the Intelligent Disaster Recovery option that needs to be purchased, implemented and configured to allow you to create a bootable recovery CDROM for your server in case of complete system drive failure. This is something you have to do before the bad stuff even happens.

If you are using a backup service like one of those three I previously mentioned, have the username and password printed out on a hard copy so you will be able to access those files and restore them over the Internet.

Keep in mind the time it may take if there are multiple gigabytes of files to restore from those remote backup services.

Bottom line: Verifying and testing your backups is just as important as dumping your data to external media so test it today.

Next week's column: CCleaner.

*John Deans of DeansConsulting.com is a Brenham area computer networking consultant who can be reached at 289-2233 or John@DeansConsulting.com for questions and comments.*