

The Bulletin

Technical Tips

By Tom Snyder Ph.D.

How to Ensure your Data is Available When You Need It

The worst time to discover that your back system isn't working is when you've lost key information and need to recover it. Nowadays, there are as many ways to back up your data as there are ways to lose it. Products range from the venerable tape back up to hard drives to online back up services. No matter which product ends up being appropriate for you, the principals of sound data back up are the same:

Determine what data needs to get backed up, how often and for how long

Keep it simple

Test your back ups

Keep some sort of back up off-site

What to Back Up The first step is common sense, yet it is frequently skipped. Conduct a thorough analysis and inventory of existing systems with a focus on data storage. A good place to start is simply by listing the directories on each server or storage device in a spreadsheet and then adding columns for the type of data in that directory (the content, not the file type—"Contracts" or "Bookmarks," not DOC or XLS), the owner (who would care if the files were deleted), and whether they are essential to your business. In a more complex environment, add another column for a time when no one is using the file and it can be backed up.

This brings up an interesting question: What *is* essential to your business? For a simple answer, ask yourself, "If I lose that file, could I lose money?" Note that the question is could rather than would; this casts a wider net—better safe than sorry.

How Often to Back Up and Keep It Simple Next consider your backup

schedule. There's a whole theory and science to backup rotations. As a result, I recommend that you skip do to step number 2 – keep it simple. The more complex your system and schedule, the greater the chance that there will be a failure.

The most simple setup is to backup everything, everyday, with very limited and standardized exclusions. Don't do incremental or differential backups. This increases the number of tapes/media required for a restore and therefore decreases the chance of a successful restore. NO "swiss cheese" backups with lots of exclusions. At some point there will be an exclusion where there should not be. If data is going to be excluded from the backup, store it in a folder called "donotbackup". Be disciplined and consistent in the spelling of this folder name and set a global exclusion for this name.

In the same keep it simple vein, get a tape drive big enough to hold all your data. Do not substitute more complicated processes and additional labor to try to make an undersized tape system work. If your data doesn't fit on one tape of the largest size (currently LTOIV = 800/1600 GB) then get an autoloader and treat the magazine as a single virtual tape – changing the entire magazine every day.

How Long to Keep Backups Save your backups for longer than you think you have to—something unexpected always comes up. (Why is it still unexpected? No one knows.) I tend to use an adapted version of Grandfather-Father-Son: I call every third Grandfather an archive and don't overwrite it. For more information on what your media rotation and labels should look like, contact me.

Test your Backups Like many of my clients, I have learned the hard way that just because you set up a job, load a tape, run the job, and even read a successful report does not mean that files were actually backed up. Tapes fail (they are mechanical), files are locked and can't be copied, and software errors do occur. Frankly, back up software is notorious for reporting that everything is satisfactory when in fact the job has failed. It is for these reasons that online back up services and hard drives are gaining ground over tapes. As a fail-safe, once a month, you should select a few files at random and restore them, making sure not to overwrite newer versions. Then open the files and confirm that they are intact and usable. A few times per year you should select a critical database, such as your email or billing database, and restore it, making sure that the

restore is usable. If you find that your restores aren't usable, you have time to address the problem before an emergency arises. Make sure that you do so.

Always Keep a Backup Off-Site The reason for off-site backup is simple: If something physically catastrophic happens at your place of work and your backups are there, they will be rendered inaccessible or destroyed. Store your off-site backup securely, in a fire proof safe or hardened facility, and update it with a current backup every day. Protecting something just long enough for someone to steal (or something to destroy) every bit of data your company cherishes is not going to help. It is for this reason that online services are preferable to hard drives.

===== If you have questions or concerns about your particular situation, please e-mail me at tpsnyder@xantrion.com. I will use your input to direct future columns. =====