PC410.COM™
Science Translations
1990 26 Years 2016

Managed IT Services, PC Consulting, Sales, & Service in Central Maryland

WHY Multiple Backups?

Is it Time to add a Cloud Backup?

This isn't the first time that you've heard me ask about your backups. Security software doesn't block new threats under three days old, surge suppressors can't handle a direct lightning strike, and no one is ready for what they don't expect. Damage to computers and your backup drives is going to happen, and there won't be advance notice.

Different backup types and destinations offer protection against different threats, and have dramatically different restore times. Some protect the newest files, and can be up and running in 10 minutes after a disaster. Others protect everything EXCEPT the newest files, from more types of mayhem, but take multiple days for recovery.

These are instructions for small business and home users; large businesses have more options, like backing up systems to virtual computers for emulation of a failed computer while waiting for IT staff to configure new hardware.

WHAT to Backup?

You should have three copies of your data, on two different types of backup (drives, cloud, or DVD/BluRay disks), and one copy should be off-site. If you're only running one kind of backup, you're not protecting your data against the most-likely problems.

Modern backup software automatically grabs your document folders. Add the contents of folders on servers, and any project folders that aren't already inside the 'my documents' folders. If you use DropBox or OneDrive for sharing files, set one system in your office to keep a full copy of those files, and include them in your backups, because cloud file-sharing isn't immune to cryptoware.

And backup these items: Software license keys (scan them), software installation disks, especially of backup software (convert them to "ISO" files and setup a folder for them on your backup drives), and the invoices that establish warranties on your computer and office technology (scan these as well).

HOW to Backup?

Image Backups are a backup against drive failures and lightning strikes. This is the backup used to rebuild your system after a drive failure–it's a snapshot of the entire drive. Some software offers this as either a drive backup or a system backup; when in doubt what a backup will do, ask the publisher.

Data Backup is a compressed copy of your data, usually documents and anything else inside the 'My documents' area, but not your software or operating system. Data Backups offer some protection against overwritten files and ransomware–there are multiple sets of data, and you can choose which to restore from.

File Sync is an automatic copy of your data. This backup saves time in getting your data running, because it can substitute for a file server, for a small number of users. Daily file sync to a network-attached storage device (NAS) is best. Continuous file sync is also an option, but that increases potential damage from ransomware, and provides no protection against human errors.

Cloud Backup, set for "continuous" backups, goes to a good service provider that keeps multiple file versions, as protection against cryptoware, and captures the most-recent files that may have changed since the last set of image backups and file syncs. Cloud backup can also save you from human errors, when you need an older version of a valuable document.

WHERE to Backup?

Cloud backups are protected from ransomware, but make sure the cloud company you choose can delete encrypted files for you, by date or by extension–ask the question, and if they can't answer in plain language, take your business elsewhere. File Sharing services like OneDrive and Google Drive are not backups; they're single-copy storage that ransomware sees as a folder that can be encrypted like any other folder. Don't use them for backups.

Network-attached storage drives are for continuous or scheduled backups. With the right software, they offer protection against drive and computer failures. If you bolt them down in a hidden spot in your building, they can protect against data loss from technology theft. Some of these units are even fire-resistant. They aren't immune to power problems, and won't survive a direct-to-building lightning strike, but neither will the wiring of your building.

USB-connected 'portable' drives (small, no power cord), and 'external' drives (larger,

with a power adapter), are for backing up and then locking up data, so they're protection against burglars and lightning, and if off-site, floods, fire, and general mayhem. But as nothing done manually is reliable, they can't be your only backup destination.

WHEN to Backup?

The standard question for backups is "How many days, hours, seconds, or months of data can you afford to lose?" Answer that, and plan accordingly. For an airline, one second of data loss is millions of dollars. For most small businesses, more than a few days of lost data may lead to financial trouble.

As a starting point for small business, try this:

- **Image backups** once a month, automated, for each computer, to a NAS drive. If your software configuration only changes rarely, an image every three months is OK.
- **Data Backups**, every weeknight, full backup once a week, and incremental (new files and changed files) for the rest of the week.
- **File Sync**, weekdays, late in the day.
- **Cloud Backup**, continuously.

On computers other than your file server, if all your data is going to the server, you can skip data backups and file sync, but in this case, create image backups at least monthly of these machines.

Keep the last three complete sets of all these backups. Assume there's corruption–there frequently is, and recovery of an older file set may be needed. In some cases, a failed backup is the first sign of hard drive trouble, so monitor the backups, and restore some files as a test. If there has been no test of your backups, you don't have any backups. Always test.

Monitor your backups. All good backup software can email the results of a backup, either that it worked or that it failed. Usually, if it fails, the backup device didn't turn back on after a power failure, or it's full. That's OK if you've got that email that tells you to check your backups.

Finally, if you've been carefully backing up for years, great! But look at the backup drive; if it's a 240 Gb drive, it could be from 2004. Backup drives fail, and old drives are slow and erratic. If you are running one type of backup, to an old drive, it's time to update. Call me for backup planning, including choosing backup software, devices, and cloud services.