Science Translations
Established 1990
PC410.COM™

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


## It’s Time to Test Backups

It’s that time of year again. When the clocks change, it’s time for safety checks, prevention updates, and disaster-recovery planning. Time to update exit plans, check smoke detectors, and test computer backups. Oh, and move your clocks one hour forward on the morning of Sunday, March 12th, 2017.

Computer backups need special attention; businesses that lose their business data tend to fail within two years. Paper trails can be useful for recreating records, but they’re rarely complete, and never in one place, or organized well enough for temp employees to re-enter them.

So planning for a data disaster can reduce risks. Here are the basics:

## Untested Backups Aren't Backups

An un-tested backup is like Schrodinger’s Cat. It’s either there, or half-there, or gone hunting, and you don’t

know which. Twice a year, restore files as a test. On every good backup system, you can restore a few files individually. For cloud backups, log into the account, and try to restore a version of an important file from a previous week. That's a fair test; half the restore help calls I receive are looking to restore the previous version of a spreadsheet that was accidentally over-written.

Try the same test for local data backups. For these, depending on the software, you may need to log into the software first, but for all of them, the steps are to explore the backups, find the file and copy it to a new folder for examination.

## Next, Audit your Office Documents

Many offices are very good about backing up their client documents, but not particularly thorough about backing up what they would need to re-build their office after a loss. Make sure that all this information is available inside your off-site backups, so that it will be there if your office is damaged somehow:

- Insurance contacts and policy numbers
- Photographs of each room and wall of your office, closeups of model/serial numbers where needed.
- Contracts, leases, and other business documents, scanned.
- Office equipment lists, with model number, serial numbers, installation dates
- Computer equipment lists.
- Software license numbers and software login user names and passwords.
- Installation software backups, either as an extra set of DVDs kept offsite, or 'ISO' copies of important software stored on your cloud backup system.
- Logins for cloud services and online software accounts.
- Finally, backup your passwords.

Preparation for an emergency includes other systems as well: The worst time to find out your uninterruptible power supplies are dead is the morning after an outage. The batteries mostly last three years; I suggest testing the units twice a year, when you change your clocks. Keep a log of the tests, showing how many minutes are available; the equipment plugged in will change the available run-time.

Backup drives age; replace them every five years, or when the computers backed up on them require more space to keep multiple sets of backups. For most offices, plan on half a terabyte of backup space per computer–that's enough for three monthly system backups, and several weeks of data backups. Exception: Offices that scan a lot, or use photographs as part of their record-keeping, will need to scale up their backup capacity based on recent usage.

## Redundancy & Duplication

Multiple weeks of data backups and system backups, plus all the information needed to recreate an office from scratch is a lot of information, and a lot of overlapped backups. These should never **all** be needed, of course. But you never know what type of emergency you could be recovering from.

- A fire can damage drives that aren't connected to power.
- Ransomware can encrypt all your data.
- A lightning strike and power surge can fry one random network box, or blow wires out of the wall.
- Burglars take random stuff, including backup drives.
- Floods happen, from storms, and from plumbing failures.

There's no one plan that covers every scenario. There's that Black Swan model again; we plan for the disasters we know about with specific steps, but for the totally-unpredictable combination of events, that Black Swan, we plan by having overlap in backups, and plans in place for multiple types of recovery.

---

## April 11th is The End of Vista

Windows Vista will reach the end of 'Extended Support' next month. That means there will be no more security patches, and no online technical assistance from Microsoft after April 11th. Existing support pages will still be available online, but will no longer be updated. Google Chrome ended support for Vista back on April 1st, 2016.

If you are still running any Vista-based computers, it's time to upgrade them, retire them or disconnect them from the Internet. Most computers that shipped with Vista can run Windows 7 faster, and many can run Windows 10. (Call for help identifying if any particular system is worth an upgrade.) And if there are still any Windows XP machines out there, it's time to melt them down. Secure erasure and safe recycling is free for my customers.

**Microsoft Office 2007** will reach the end of extended support October 10th of 2017. If you're running Outlook 2007, plan ahead. Running an unpatched email program isn't safe. Now is a good time to switch to Thunderbird.