

Minimizing Pain Dept.

Choosing The Best Backup Strategy

By Mark Costlow, President

Tax time provides a good opportunity to remind everyone to do data backups. Many people don't back up their files at all, and they occasionally pay a high price for that. But what if you have been diligently making backups and it turns out they aren't useful for the particular calamity that befalls your data? That's a very painful sucker-punch – as if you've been paying your insurance premiums for years only to have coverage denied when you most need it.

Let's assume you already are aware of all the reasons why you should regularly back up your data. How do you decide what strategy to use? There are quite a few options now available: tapes, DVDs, USB hard drives, flash drives, online backup, and more. Which is best, most reliable, easy, and convenient? Should you use more than one?

First, let's consider the four major causes of data loss: **crash**, **corruption**, **theft**, and **disaster**.

Crash: In the early days of computing, hard drive crashes were common. Since the 1980s, they have become extremely reliable. Many people have never experienced a crash, but they still happen. It may be possible to recover some or all of the data from a hard drive crash. However, it requires an expert with specialized tools, can cost thousands of dollars, and takes many days or weeks.

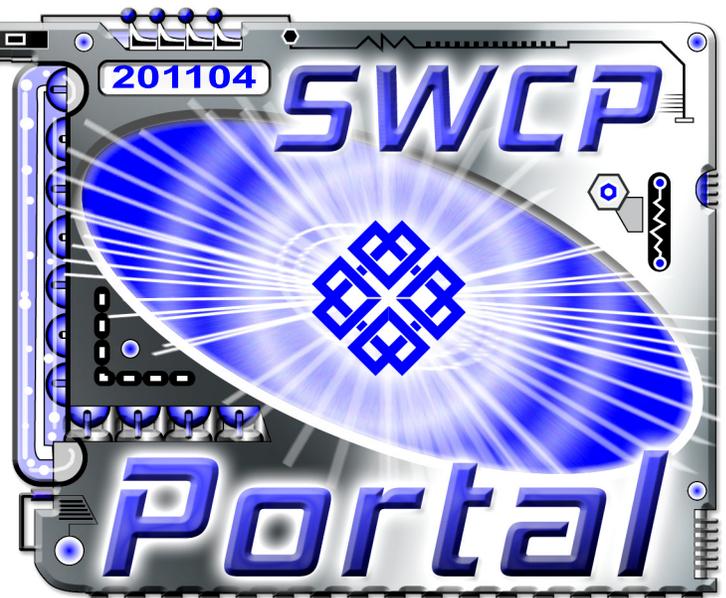


One way to protect against hard drive crashes is to use "mirrored" drives, where every file saved is written to two hard drives at the same time. If one dies, the second drive continues to work until the failed drive is replaced.

However, this is not a complete backup strategy, and fails to address some of the possibilities involved.

Corruption: Corruption is any mishap which renders a file useless. Some typical examples are:

- Accidental deletion
- Operating System failure
- Application program bug
- Power failure while saving a file



- Accidentally saving changes, overwriting old information

The disk mirroring strategy described above does not help in this case. If you delete a file by mistake, it gets removed from both disks at the same time. Many systems can recover a deleted file if you notice right away. But what if you accidentally delete a page from a spreadsheet and then save it? Both hard drives have the "bad" data saved and you can't get back the deleted portion.



Nightly backups of all your files to an external hard drive can help, but you'll just have a few days to realize the problem before the old data is overwritten.

To protect against corruption, you need to have "generational" backups, meaning that your backup has more than just one "current" copy of your data. Ideally you would like to be able to recover any previous version of a file, going back months or years. Realistically you have to balance this against the cost of saving that much data. Some online systems excel at this feature as does the **Time Machine** system built into Mac OS.

The downside of **Time Machine** is that if you use it on a machine with only one disk, your backups will be on the very same disk as your live data. So while you have many generational backups to protect against corruption, there's no protection against a disk crash, or the physical loss of your computer.

Theft: Having your home or business burglarized is a terrible experience. Thieves zero in on items that have the highest value per pound. That means computers, especially laptops, are prime targets.

Continued on back



SOUTHWEST

CYBERPORT swcp.com | help@swcp.com

New Mexico's Leading Local Internet Service Provider

5021 Indian School NE, Suite 600, Albuquerque, NM 87110-8910 USA

505.232.7992



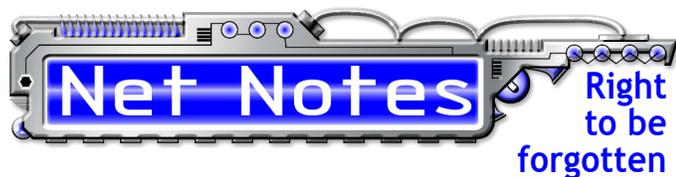
Many backup strategies are useless in the face of theft. If the backups are on a second disk drive, they will likely get taken with the computer. With tapes or disks, you may be able to recover, especially if they are stored in a separate location from the computer.

A significant issue to consider in this case is how long it will take to recover your data. If you have a tape backup system, do you have a spare tape drive? The pile of tapes in the safe or the back room are not much use if the only tape drive is stolen with the computer. And did you remember to label each one?

You really need to maintain physical copies of your backup data off-site. Arrange to store tapes or hard drives in a separate secure location. Remember that your home or business insurance policy may cover the computer hardware, but it almost certainly excludes the data. The irony is that your data can be worth a thousand times more than the computer hardware it's on. And some data is simply unreplaceable, such as digital photos of a deceased family member.

Disaster: The "Disaster" category includes any natural or human-made physical catastrophe. Fire, earthquakes, floods (natural or plumbing-related), car accidents, and other disasters can all leave your computers in shambles.

As with theft, protection against a physical disaster requires keeping offsite copies of your data. A backup regimen of regularly taking copies of the backups to another location will accomplish this. In a small business, that often means one of the company principals takes tapes or disk drives home each day or week. If the data is extremely sensitive, you can store it in a safe deposit box at a bank. Home users can simply trade storage of tapes or CDs with a trusted friend.



The European Union is about to enshrine a new human right: "the right to be forgotten online." In a speech to the European Parliament, Justice Commissioner Viviane Redding warned companies such as Facebook that they must comply with EU rules. In a package of proposals to be acted on this summer, she intends to force Facebook and other social networking sites to make high standards of data privacy the default setting, thereby giving control back to users.

She proposed that people should have the right to withdraw consent to online data collecting and processing and that data gatherers would have to prove they need the data.

- The Guardian, UK



Online backup services also meet this requirement. Most online services will allow you to restore your files to any computer, from any location, as long as you have the password required access the files. The key is to get the data outside your facility so that it is not all in one place.

Any system, or combination of methods that you use to back up your data, should not only be secure, but as simple and automatic as possible. It takes discipline to remember to change tapes or disks each and every day, and it can be very tempting to forget or blow off. The best system would automatically store your information in a secure, off-site location, or even better, several, on a routine cycle of your own choosing.

Such a system would be incremental – only incorporating changed data – and generational – saving older copies in case you make accidental deletions. The system would be easily accessible with a password from any web browser, and support encryption. And it would work with any operating system over your own broadband connection at your own convenience.

Southwest Cyberport's own online Backup Service, the **SWCP BUS**, does all this and more. *Just set it and forget it.* The BUS provides reliable, secure, and easy-to-use software to back up all of your important files online. Available for individual users or your whole local network, "seed loads" with portable drives can make initial set-ups a breeze, even with huge data sets. We also offer a special low-cost online data locker just for students, the **SWCP SchoolBUS**.

Check out <http://www.swcp.com/bus> for details.



Free Internet Class

After a long hiatus, SWCP's popular "Introduction to the Internet" class returns, covering the basic features of the latest versions of Thunderbird and Firefox, the popular open-source email client and web-browser from Mozilla. It's free to SWCP member customers, but space is very limited, so sign up today!

Introduction to the Internet is only offered on Saturday, May 7, 2-4PM in our classroom.

Make your reservations by calling 505-232-7992 or emailing Tech Support at help@swcp.com

