

Backup Critical Files



The day after the 2001 terrorist attacks against the United States we reviewed our organization's data backup procedures to be sure that we were properly protecting our most important asset: our computer files. We needed to be prepared to resurrect operations at a new location if we had an emergency. What we found shocked me.

What we were doing

We were carefully duplicating the data on our primary servers to the backup servers each day, making digital images of all workstation hard drives, and securing CD backups of all our encryption codes and website files. We even had removable hard disks in our servers and frontline workstations so that the drives could be easily removed and carried from the office if we had to evacuate.

What we failed to do

What we weren't doing was moving any of this data offsite every day. If our office were destroyed by a disaster, man-made or natural, and we weren't able to pop the removable drives, we would lose all of our computer files.

How we improved

That Wednesday afternoon, September 12th, I ordered an external hard disk for the workstation closest to the exit door. The drive connects via a FireWire (IEEE 1394) cable and automatically maintains a copy of all data files on the primary servers as well as the digital images of our most important workstations. The drive is the size of a pack of 5x8" cards and weighs about a pound. It's hot-swappable: it can be installed or removed while the workstation is running.

It can be plugged in, the backup executed, and then removed. I'm responsible for this routine, and I keep the drive in a secure storage container in my car. The hard drive only stays in the building for the two minutes it takes to run the backup procedure.

Take data offsite

It's vital that computer files are stored securely. Storing backups next to the server won't do a bit of good if the office burns in a fire or if it's burglarized.

Our post-attack security analysis also included reviewing our business insurance. Fortunately all of our computers and data systems were properly documented and insured; however, none of our data was insured. Let me beat the drum once more: we (and you) need to backup the computer files and move them to a secure offsite storage location every day.

Why not tapes?

We no longer use digital tapes to hold our computer files because, quite honestly, they were a pain in the neck. The daily backups were taking over eight hours to complete, which meant that we couldn't work late into the night

without affecting the backups. The tapes often proved unreliable. More than once we couldn't recover a file because the tape had a read error that wasn't caught by the backup software's verify procedure. We changed tape hardware and software three times: each brand proved equally unreliable.

What about CDs?

For a few years we burned data to CDs but as our networked data grew, we needed more and more CDs to store the data. When we reached 10 CDs a day, I called it quits for that strategy.

We had the most reliable backups when we installed duplicate servers that automatically copy data from the primary servers. All data files are also copied to removable hard drives installed in a few, select workstations. Sensitive files are encrypted before they're moved to the removable drives.

Our most critical asset, our computer files, are also the only asset that can't be insured.

How well do removable drives work?

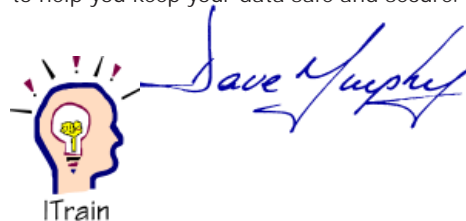
Since installing the removable drives, we've never been unable to restore a file. Our backup software has the option to purge unneeded files from the backup drives, and we rotate multiple drives to keep a short-term history of all file changes.

To maintain a longer history of changes to databases, we selectively use CD backups. These CDs are then stored in a specially-designed heatproof safe that will protect the CDs in the event of a fire.

Final thoughts

The backup procedure you employ doesn't have to mirror our procedure. If you're having good luck with your tapes or CDs, keep using them; just make sure you're moving them offsite every day.

If you'd like more information on our procedures, drop me an e-mail note. I'm glad to help you keep your data safe and secure.



ITrain
International Association of
Information Technology Trainers

6030-M Marshalee Dr PMB 616
Elkridge, MD 21075-5987
410.567.5366 or 888.290.6200 or
801.650.0423 (fax)
itrain.org member@itrain.org