Why You Need to Back Up Your Data

Angus B. Grieve-Smith
April 17, 2006

Nobody likes to do backups. It's like flossing your teeth. But as with flossing, you can run a big risk by neglecting your backups. In this article I will describe a number of things that can (and will) go wrong with your computer system, and suggest some ways you can protect your data. In other articles I will suggest specific steps depending on your situation.

When a Hard Drive Breaks

All hard drives break. The hard drive is one of the major moving parts in the computer, and it's spinning constantly. Your hard drive *will* break; it's not a question of "if" but "when." There are two ways to protect your data: **backups** and **mirroring**. A backup is a copy of the data that is made on a regular basis, usually every night. A mirror is a duplicate hard drive that is updated almost immediately after changes are made. Mirrors are a bit more expensive than tape backups, but they allow you to keep working while the faulty drive is replaced. If there is no mirror, the restore may take several hours, and all of the changes since the last backup will be lost. Because mirrors don't protect against other risks, many organizations use both backups and mirrors.

When Someone Accidentally Deletes a File

If you've been working with computers long enough, you've seen people delete files by mistake, files that they (or someone else) may have spent hours or days creating and editing. Backups can protect against accidental (or malicious) deletions; individual files can be restored from the last backup. Another strategy is **snapshots**, where the operating system keeps copies of all deleted or changed files for a given period of time; users can simply look in the snapshot directory and retrieve earlier versions of the files.

If You are Audited or Investigated

Some regulatory agencies require **archives** (particularly of financial records) to be kept for a period of time. Archives can also be useful for court cases, or (on a more positive note) historical record. Backups can provide these archives, simply by keeping the backup media rather than overwriting it.

If Your Office is Destroyed

We hope this will never happen, but it makes sense to plan for disasters like this. If your backup media are stored in the same place as the original data, they may be destroyed as well. To help your organization recover quickly, you can periodically store some of your backups **offsite**, either at an offsite storage facility or someone else's home.

Angus Grieve-Smith is an independent computer consultant. More information can be found at <http://www.grieve-smith.com/> or contact Angus by phone at (718) 205-8665.