

Learn-IT Newsletter for the month of May (published May 2, 2003)

An Ounce of Prevention: What to do Before and After a Computer Disaster

by Mark Flores, MCP, MCSE

Here's a simple question for you: How would your life be impacted if all the data on your computer was suddenly lost right now? If this question just sent a chill down your spine, then this article is for you.

Death, taxes and computer crashes. We will all experience these inevitabilities at some point. "It's not a matter of *if*, but *when*." This familiar phrase is especially applicable to our computers and the important data that they contain. Surprisingly, many companies have no disaster prevention plan in place whatsoever. Is yours one of them?

What you should do before you have a computer disaster:

1. **Backup your important files.** Sounds obvious, doesn't it? If you have important work on your personal machine, burn a copy of it to a CD once a week. If your company has a server, be sure that it is backed up on a daily basis to a tape drive or other mass storage device.
2. **Have a backup strategy in place.** Your company should have a written description of what you backup, when it is backed up, how often it is backed up, and who is responsible for changing the backup tapes.
3. **Monitor and test your backups.** Make sure that your backups are viable by checking the backup log regularly and periodically restoring a few files to an alternate location.
4. **Save your data to a network drive.** Most companies have a backup device for their server, but not for each individual workstation. If you have been allocated some storage space on your server, place your important files there so they will be added to the daily server backups.
5. **Invest in Fault Tolerance.** (see below for an explanation)
6. **Schedule regular disk scans and defragmentations.** Your operating system has built-in disk scanning and defrag software. Use the task scheduler to automate weekly maintenance.
7. **Consider offsite backup storage.** If your building burned to the ground overnight, could you still recover your data? Take one backup tape home each week, or store your backups in a fire-proof safe.

A computer disaster usually occurs when one of two things happens – either your data has been lost due to a media error (it gets erased or corrupted, for example) or a physical problem (hard drive or computer goes bad).

What you should do after you have a computer disaster:

1. **Determine if your data loss is due to a physical problem or a media error.** If you can still access the drive where the data used to be, then you have a media error. If the drive is dead, or if you can't access any of the data on the drive, then you most likely have a physical problem.
2. **Replace the faulty hard drive and/or restore the data from a backup.** This is the easiest solution, but assumes, of course, that you followed the steps above.
3. **Seek professional advice and help.** There are a number of free resources that you can download from the internet or purchase at your local computer store, but when you decide to do-it-yourself, you run the risk of corrupting (or even losing) your data. Use these programs at your own risk.

Now it's decision time. Is the lost data worth the price of having it professionally recovered? Data recovery specialists have facilities for dismantling your hard drive and meticulously retrieving the raw data from your media. Unfortunately, this procedure can cost anywhere from \$500 to \$3000+ depending on the amount of data you need recovered. Ouch. (After you finish reading this article, why don't you backup those important files just to be sure, okay?)

Relevant Terminology

Fault Tolerance – Fault tolerance is an investment in redundant computer storage. For example, if you have a hard drive that goes bad, a second (redundant) hard drive will take over until you can have the defective drive replaced. There is no loss of data, and more importantly, no downtime for your network.

RAID – A method of fault tolerance called RAID (Redundant Array of Inexpensive Disks) offers several options for redundancy. The two most common are RAID Level 1, where all of your data is mirrored on two separate storage devices, and RAID Level 5, where data is spread out over three or more hard drives. Each of the drives keeps

redundant information about the other drives in the array, so if one hard drive goes out, a new one can be added and the data is regenerated from the remaining hard drives in the array.

Backup vs. Fault Tolerance

A question I hear often is, "If I have regular nightly backups, why do I need to spend more money for fault tolerance?" This is a very understandable question, but there is a difference between the two. It's easiest to describe this with examples.

Example #1 - **Your hard drive goes bad, but you have a backup.** You need to replace the drive by either purchasing it locally, or ordering it from a manufacturer. Once you get the drive and install it, you may have to reinstall the operating system and then restore the files from backup. This can easily take the better part of a day or longer to complete. During this time, your computer is down, and if this is your company's server, most likely your company is down as well.

Example #2 – **Your hard drive goes bad, but you have fault tolerance.** When the drive fails, you (usually) get a warning that there has been a hardware failure. At this point, everything continues to work normally since the redundant drive has taken over with duplicate data. Later, when you get a replacement for the bad drive, it can be re-incorporated back into your fault tolerance system.

Example #3 – **Someone on the network accidentally deletes an important folder from the server, you have fault tolerance, but no backup.** Since fault tolerance keeps an up-to-date copy of your data on redundant drives, when that person deleted the folder, the redundant drive also deleted its data. Therefore fault tolerance can not help here, only a backup will be able to retrieve the deleted data.

The best solution, of course, is to have both systems in place. While backup alone will provide protection from data loss, fault tolerance will keep your company operating at all times, with no loss of productivity.

Mark Flores is a Microsoft Certified System Engineer and President of Infinity Networking, Inc. Mark has taught computer certification courses at Maric College, served as IS manager for a San Diego biotechnology company and is a former high school teacher with over 22 years of computer experience.

The *Learn-IT* newsletter is published once a month by [Infinity Networking, Inc.](http://www.infinitycorp.com) To subscribe to this newsletter and have it e-mailed to you automatically, send an email to news@infinitycorp.com. You can opt out of the newsletter at any time. Please feel free to forward this article to anyone who may find it of interest.