

Why Backup?

"What, me worry?" - Alfred E. Neuman

One of the things that I harp on the most about when it comes to preventive maintenance and system care is the importance of regular, reliable data backup. No matter how well you treat your system, no matter how much care you take, you cannot guarantee that your data will be safe if it exists in only one place. The risks are much greater than most people realize.

How important is your data to you? You can respond to this question with words, but the steps you take to protect your data are the real answer. I find it troubling when people lose large quantities of data--because they have no backups--and then they get very upset, talking about "how important that data was!" If it is important, why was it not backed up? If it matters enough to get upset over losing, it is worth protecting, and backups are an essential part of data protection.

There are many reasons that people neglect doing backups:

- They do not understand how important they are, because they have not had a disaster happen to them - **Yet**.
- They do not know how.
- They forget to do them because they do not have a routine for doing backups.
- Doing the backup is a time-consuming chore and they cannot be bothered.

This article takes a full look at the importance of your data and why you should backup.

A Mental Exercise To Underscore the Importance of Backups

Most unfortunately, there are some things that people only take seriously after they have experienced personally the pain that results from not taking them seriously. Backups definitely fall into this category. Most people are relatively nonchalant about them until disaster strikes--thereafter, they are much more diligent about backups (but after the damage is done.) Despite the difficulty in getting people to learn from others' mistakes, I am stubborn, so I will try anyway in this section)

Here is a mental exercise that you can do to help you understand how important backups are. Take a look at your PC and think about what is on it. Think about your data and your programs. Consider how much time it took to create the data, and to set up and tweak your PC so that it works the way you like. Now imagine that one morning you go to your desk and the PC has vanished without a trace. What will you do?

Let us suppose you had insurance on the hardware, and a week later a new PC shows up at your door with a fresh new, *clean* hard disk. Now what? Most people, who ask themselves this question seriously, begin to take backups much more seriously. (Fortunately, for most people the exercise is only a mental exercise, but don't think it cannot happen to you in the real world.)

Recovering from a disaster such as a total disk crash or theft of a PC box can be a very traumatic event, much more than most PC users realize. This is true even if backups exist; when they do not exist, the situation is much, much worse. The pain of recovering from a disaster is almost always very high, and the cost is primarily in the time required to recreate the lost data. For even a small business, this can run into the thousands of dollars very quickly.

If you still are not convinced, consider this report from the University of Texas Center for Research on Information Systems. Of the companies that lose their data in a disaster:

- 90% are out of business within two years...
- Nearly 50% never reopen their doors at all after the disaster!

The Risks to Your Data

If you do any sort of reasonable amount of computing, it is only a matter of time before you some day need access to backups of your data or programs. There are many different risks to your data; most people just think of the infamous, dreaded disk crash. This is a real risk due to the technology used in data storage, but there are many other ways that you can easily lose data on your PC. In fact, the list of risks below is far from exhaustive, though it covers the most common problems.

Some backup methods protect against all of the risks below, while some protect only against one or a few of them.

Hardware Failure

The risk of hardware failure is the most commonly talked-about reason to perform backups. Indeed, nothing will jolt someone into realizing the importance of backups more than an unrecoverable hard disk failure. Since the hard disk stores your main programs and data, it is the hardware whose failure hurts the most. It is also what gets the most attention, and rightly so.

However, there are other hardware problems that can cause permanent data loss, and some of these can be rather hard to figure out, since they don't seem like they should be responsible for the problem. Here are just a few:

- **Memory Errors:** With so many systems today running without error detection or correction on their system memory, there is a chance of a memory

error corrupting the data on the hard disk. It is rare for it to happen, but it does happen.

- **Resource Conflicts:** Conflicts resulting from peripherals that try to use the same interrupt requests, DMA channels or I/O addresses, can cause data to become corrupted.

- **Power Loss:** Losing power at the wrong time, such as when you are doing sensitive work on your hard disk, can easily result in the loss of many files.

Software Failure

It is possible for data to be lost due to software bugs, or even just poor software design. For example, a program might have a problem where it crashes upon saving a file. Many programs, when saving a file on top of an older file with the same name (such as when you select "Save" to update the current document you are working on) will first save the new file under a temporary name, and then rename it to the correct file name when the save is completed. But others may remove the old file first, so that if the software crashes during the write process, the old file will be lost as well.

Some software bugs may be even more damaging, even causing the loss of files unrelated to them. This does not happen very often, fortunately.

File System Corruption

There are many ways that the file structures used to contain programs and data on the hard disk can become damaged. In some cases, this corruption can result in data loss, especially if the disk is not maintained properly and the file system scanned on a regular basis.

Accidental Deletion

Since computer users are human, they make mistakes. One of the most common is accidentally deleting files from the hard disk. There are many different protection mechanisms and "undelete" utilities that can help recover from this, but sometimes you delete a file and then remember a few days later that you really need it, and in this situation a backup is often the only thing that can save you.

There are other ways that you may accidentally delete files, maybe without even realizing it. Of course being careful can avoid this sort of problem (be sure of what you delete!) but a backup can save you from the occasional accident.

Virus Infection

Viruses can easily cause the loss of data, in many ways. This includes loss caused directly by the virus and also program damage that results from efforts to remove viruses from a system.

Virus Detection and Protection

There was a time when you only had to worry about you (and your family) screwing up your own PC. Now you have to worry about complete strangers doing it for you. Due to the nature of how software works, it is possible to write programs that can modify or create other programs--a compiler is one example. It is also easy to duplicate a piece of code and write it to various locations on a hard disk. It did not take very long for some ingenious--but perhaps diabolical--hackers to figure out that they could write pieces of software that would do these things and more, without the user's knowledge or consent, and the virus "industry" was born.

While viruses have been around almost as long as the PC, they have only recently, within the last few years, changed from minor inconvenience to serious menace. There are several reasons why they are now much more of a problem: many more computers are in use, and there are many more ways of sharing information between them. Advances such as the Internet have made it possible for computer viruses to spread much more quickly than ever before, and more computer users in general--especially those that do not understand what viruses are--have given virus writers a much richer set of targets.

Theft

Many PC users do not consider the possibility of theft as a danger to their data (although most people who use notebook PCs certainly do!) Even for desktops, there is always the risk of the entire PC box disappearing one day if you have a break in, for example. It is important to keep this possibility in mind, as some kinds of backups do nothing to protect against theft. To my knowledge, insurance that covers theft of computers will allow you to replace the system, but cannot pay to recreate lost data.

Sabotage

Generally applicable only to PCs in the work environment, sabotage by disgruntled employees is a growing problem. A carefully constructed backup program is the only protection against a knowledgeable but angry person who is determined to intentionally cause data loss (and sometimes, even backups are not enough.)

Natural Disaster

Fire, flood, earthquake, mudslide, hurricane, lightning strike, you name it: all can result in the destruction of your PC and everything on it. For many people getting back their data will be the last thing on their minds when this happens, of course. For others, getting back up and running on a PC may be something they need to do right away.

Remember that insurance may cover your PC's, but it will not cover the data!