What You ***Must*** Know About Backing Up Your Computer

By Jeff Bell
jeff@MyHealthOptimiser.com

It may seem strange for me to be writing about computers and information technology. After all, I am a health researcher and practitioner, right? Well, what some may not know is that in addition to my decades of health work, I've also spent years providing information technology consulting to a host of business clients, both large and small.

And I run a fairly sophisticated computer network to support my health work and research and to support the content for our web site: www.MyHealthOptimizer.com.

If you are having trouble making the leap, think of this as health advice for your computer.

One disclaimer before I launch into the details: All of my work has been on the PC platform. I have very little experience with Mac technology. The detailed advice I provide in this article pertains to Windows PCs and not to Macs. However, many of the basic principles still apply.

Let's get started – First Principles:

Which Kind Are You?

There are two kinds of people who use computers: People who back up their data and people who lose their data. There are no known exceptions to this law of computing. If you do not back up your data sooner or later you will lose it. I guarantee it.

I speak from personal experience. When I first started working with PCs I arrogantly decided that since I was an "Information Technology Professional", I did not need to worry about losing my data. I got away with this for about a year. Then Murphy paid me a most unwelcome visit.

I have been fanatically meticulous about backing up any computer I work with ever since.

What Is A Computer Backup?

Simply put, a computer backup is a copy of all or some of the data that is stored on your hard drive. Typically, such a backup or copy is stored on another device. This protects you in the event that your hard drive fails. It also offers protection against a number of other common computer mishaps:

- Accidental file deletion
- Virus or other malware infection
- Software version and installation problems and errors

- Computer theft, fire or other hardware destruction
- A myriad of other errors and mishaps

These days the two most common ways to implement such protection are to use special backup software to copy the data onto an “external hard drive”, (these are typically connected via a “USB” port), or to copy the data to a remote location via the Internet.

There are a number of remote location backup services available. These are known as “on-line backup services” because the copy is literally transmitted, on-line, over the Internet, to the storage facility. This has the advantage of allowing you to keep a copy of your data in a location that is secure and that is physically distant from your computer. If there were a fire or other disaster that damaged your computer, the data would still be safe and retrievable in its remote location.

The disadvantage of the on-line services is that the good ones, (reliable ones), are typically expensive on an ongoing basis. If you have a relatively small amount of data to protect, this may not be a problem, as they generally charge based on the amount of data to be transmitted and stored. Another potential disadvantage in using certain services is that some may take quite a while to provide you access to your data in the event you need to recover your data.

If you do use one of these services, then be sure they provide a way that you can log onto your backup service account remotely and recover single files, or small groups of files without requiring their intervention and without incurring extra costs. This is really handy when its 3 in the morning and you realize that you just accidentally deleted the appendix to your doctoral dissertation that you spent the last 3 days writing!

For many computer users an external hard drive that connects via USB may be a better choice. These have recently become available with very large storage capacities at reasonable prices. Personally, I prefer the Seagate brand drives for this as they seem more reliable than most of the other brands. They typically are slightly more expensive but I think it is worth it.

Local Or Remote? Best Of Both Worlds:
I really like the convenience of having immediate access to my backups. So I backup to external storage devices that are here in my office. But I also want the security of knowing that my data is safe, and that there are recent copies of it in another physical location.

To have the best of both worlds I have a couple of extra, large-capacity external hard drives. Every day I back my data up onto a large external storage unit. (I have a full network, so just USB drives would not be sufficient in my case.) Once each week my backups get copied onto one of my external USB drives, which then gets sent off-site. Each week I rotate the external USB drives so that the newest set of backups is being sent off-site and the oldest set is being returned to be overwritten with the next week’s data.

What Needs To Be Backed Up?
There are people I know who just backup their actual data. What I mean by that is they only backup the files they are working on. For example, one of my colleagues writes lots of articles in Microsoft Word. He only backs up the actual articles that he has either finished or that are in progress.

In my opinion this is a mistake. Think about how long it takes to reinstall Windows, reinstall all of the software that you use, and then the hours to configure everything. What a colossal waste of time it would be to have to redo all that work!

To me that is far too much risk. To protect myself against all that potential lost time and productivity I back up my entire computer, Windows, all of the installed software, the files I am working on, in short, everything. And that is what I recommend for most computer users.

Weeklies and Dailies:
Once each week I make a full backup, which includes every single bit of data on my computer – Windows, software, configurations, work product files, etc. This "Weekly Full Backup" includes the whole computer, regardless of whether the files have been changed since the last backup or not.

Each night in between my Weeklies, I make a Daily backup. This Daily backup includes all files, (including software and configuration files), that have changed since the last Weekly backup.

Windows makes this easy to do. The file system under Windows keeps track of which files have been changed. Each time I make a Weekly or "Full" backup, Windows resets the flag that tells the backup software that the file has been modified.

For example, let's say I make a Weekly backup on Sunday night. Then during Monday I edit two Word documents, 1 Excel spreadsheet and install an upgrade to Adobe Acrobat Reader. My Monday night Daily backup will include all of the files that I have changed during the day. It even includes the parts of Windows as well as any configuration and user settings files that have been modified by the Acrobat upgrade.

The specific type of Daily backup that I use is called a "Differential Backup". This simply means that each Daily backup is cumulative – it backs up all files that have been changed up to the time the backup is being made since that last Weekly, full backup. These "Differential" Daily backups do NOT reset the flags. So a file that was changed on Monday gets backed up that night, then it gets backed up again on Tuesday night even if it has not been changed since Monday. In fact, it continues to get backed up each night even if no further changes are made to it, until the Weekly "Full" backup. The Weekly "Full" backup resets the flag so that the file no longer is included in Daily backups until it gets changed again.

At first blush, it would seem that this is a lot of redundancy because the Dailies end up backing up some files several nights in a row even when they may not have been changed each day. That is true. But there are complex reasons, having to do with how Windows works behind the scenes, that make this the preferred strategy for effectively protecting yourself from loss.

Some people employ “Incremental” backup for their “Dailies”. I do NOT recommend this strategy. True, it saves a little bit of space on your external drive, and it saves a small amount of time to make the backup. However the price you pay for those savings is a significant decrease in protection and a big increase in overall risk. To me, the savings do not justify the increased exposure.

Software For Backups:
If you had to create the backups, either Weeklies or Dailies, by hand, that is keep track of the files you need to back up and then copy them onto the external hard drive or send them to your on-line service, it would take too much time and work to be practical. Fortunately, very good software is available that automates creating your backups, as well as helping you recover should you need to.

Many of the external hard drives that are sold come with free software for making backups. I do NOT recommend that you use it. It is worth what you paid for it. I would not even bother to install it.

The newer versions of Windows also include utilities for creating backups. Some of these built-in utilities are almost good enough, almost but not quite.

I recommend that you purchase dedicated, commercially published software that you install on your computer to make your backups. There are a number of backup software products to choose from.

My personal favorite as of this writing is: Acronis. I use Acronis ABR10 Workstation to backup my Windows 7 workstation. Acronis is reliable, fast running and has good technical support should you need it. They publish a standard version and an advanced version. For most users the standard version is all that’s needed. Further, it is less expensive and much simpler to install and configure. As of this writing costs for the Acronis ABR10 Workstation software range from $50 to $80, depending on whether or not you include a special feature called: “Universal Restore”.

I love Universal Restore because it allows me to take an entire backup made on one computer and restore it onto a completely different computer. If my laptop died it is too old for me to be able to replace it with an identical laptop. That model is no longer available. However, if I have Acronis with Universal Restore, I could restore my backup onto a completely different laptop, or even a desktop computer and be quickly back to work. (Different computers use different system files called: “drivers” and with most backup software these differences make it impossible to restore a backup made on one computer onto another computer that is not completely identical, hardware-wise.)

Here's another feature I love about the Acronis backup software: Acronis makes a "disk image". It literally makes a "snap-shot image" of your hard drive. This means that you can restore an Acronis backup to a "bare hard drive". With most backup software, if you have a serious failure, such as a hard drive crash, you need to replace the hard drive, then re-install Windows before you begin recovering your data. Not so with Acronis. If my hard drive fails, I buy a new one, install it and let Acronis take the recovery from there. I do not need to re-install Windows or any of my software. Acronis will do it all from scratch.

Acronis also has a good scheduler built in. I have mine set to create my Daily backup each week night and my Weekly backup each Saturday night.

How Long Do I Need To Keep My Backups For?
That is a hard question to answer without knowing more about the nature of your work. However, here is a good general principle to follow: Try to keep a minimum of 4 complete generations of backups. That is, I would have at least 4 Weeklies and all of the Dailies that were made in between. If you have capacity to keep more there is no harm in that. I keep 8 generations of backups so I can always go back two full months to grab data that I may have not even realized I lost at the time. That has saved my backside more than once.

Again, Acronis to the rescue. I am glad that I do not have to remember to delete my old backups. If I were to forget to delete my old backups, my external hard drives would soon run out of space. Acronis allows me to set a "retention period". It then automatically deletes backups that are older than the designated time period. I consider this an essential feature of any good backup system.

Special Backups:
There are special sets of files and data that I keep "forever". At the end of each fiscal year, when I close my books for that year, I make a special backup of my financial data, burn it onto a CD or DVD and store it for as long as my accountant says we need it. This is generally for the same period of time that she recommends we retain tax records. I make several copies of these special backups, keeping 1 in my office, 1 in our fire-safe, and 1 in a safe deposit box at the bank.

How Much Insurance Do You Want To Buy?
Backing up your data is a little like buying insurance. It is possible to invest quite a bit in protecting your data. But you may not need to. Just as in making an insurance decision, you assess the risk, estimate the value of what you are insuring, and base your decision on those factors.

With these considerations in mind you can decide how much effort, time and money to devote to protecting your data. (Keep in mind that you are also protecting the system that you use to do your computer work, not just the data.)

Generally, the more time and effort it takes to create the work in the first place, and the more it would take to re-create it from scratch, the more it is worth spending to protect it.

If your data and your computer work is at all important to you I recommend that you consider retaining a qualified computer technician to help you get your backup system installed and configured. For most workstations this should not require more than an hour at most.

There are many strategies for backups, and lots of different approaches. The principles explained in this article have stood the test of time. I have relied on them myself as have many of my clients over many years of consulting in the information technology world. So if you do retain a technician to setup your backup and data protection system you might ask them to skim through this article to be sure they are following the basic concepts and getting you appropriate protection.

Please feel free to send your questions or comments to: jeff@myhealthoptimizer.com

To your great health!

Jeff Bell

Please visit www.MyHealthOptimizer.com for more valuable health information.

Disclaimer: (Note my re-purposed disclaimer. How's that for efficiency!) Please note that the information in this document is provided for educational purposes only. This document is not intended to diagnose, prescribe or otherwise provide specific recommendations in relation to specific ~~health~~ computer problems. It is not intended to take the place of the services of professional ~~and/or appropriately-licensed health care providers~~ technicians. The statements made in this document have not been evaluated by ~~the FDA or any other regulatory body~~ anybody other than my cat. If you have a serious or potentially serious ~~health~~ computer ~~condition~~ problem, it is recommended that you consult a qualified ~~health care provider~~ computer technician. The author of this document invokes the First Amendment of the Constitution of the United States of America and specifically the rights to free speech guaranteed therein. The contents of this document are his legal free speech expression according to those rights.

Copyright © Jeff Bell / www.MyHealthOptimizer.com – 2011 – All rights reserved.
This article may be copied and/or freely distributed, as long as the doctrine of "Fair Use" is maintained in the course of such distribution or re-distribution. It must not be altered without the written consent of the author, Jeff Bell. Compensation, monetary or otherwise must not be required as a condition of its distribution or its receipt.