Disaster Recovery for your Computer System

Originally appearing in THE PICTURE PROFESSIONAL 2006 Issue 3
American Society of Picture Professionals

Has your PC experienced the dreaded blue screen? Has your McIntosh suddenly emitted a screaming of brakes followed by a sickening crash?

If you haven't yet been terrified by one of these events or a beheld a bewildering monitor display of hexadecimals with an error message, you either haven't been computing very long or you've been very, very lucky. All computers can be expected to crash and burn at some point in their life cycle. There will be some data loss. In most cases, it won't be horrific.

The first rule is: Don't Panic! You didn't do anything. Most errors are recoverable.

The second rule is: Computer programmers are sadists with sick senses of humor. Witness the scream of brakes and the crashing sound on the Mac. Don't panic!

I once had a machine where an error sounded like liquid sloshing around inside, followed by the sound of water draining faster and faster until finally everything went down the drain. Rule number two! Ha! Ha! Ha!

What's going on?

Imagine a formless void inside your computer where little characters called bytes speed about in cyberspace. Like in outer space, some of these little byte do-dads collide. This knocks them off their planned trajectory. The processor chip inside your machine is supposed to track the bytes that are actually not bytes at all but composed of still smaller felons called bits. A bit is an on or off impulse. The absence of an impulse in a timing sequence is considered an off by your computer processor.

Now, all bytes are divided into two parts; a zone and a digit. Each is composed of four bits. Half a byte is called a nibble. Remember rule number two! Programmers have a sick sense of humor. Apple even named its computer magazine Nibble.

Anyway, bytes collide like meteors in space and the processor chip has become very confused. A particular byte was expected to be found at a special location in memory but has ric-o-shayed off into cyberspace. The processor chip becomes momentarily depressed or a little blue and so is your screen. Again, remember rule #2.

The point (other than to have a little fun explaining it in very general terms) is to remind you that you haven't done anything. You are not a bad person. Computers crash. Your job as a superior being is to prepare for the inevitable and reduce or eliminate the collateral damage.

Disaster proofing your computer system:

Your first line of defense is a power strip. A little power spike can start to cause all those byte thingies to begin colliding and foul up the timing sequence the processor is expecting to see.

Sometimes, a little surge can leave a residual charge that can require

you to open up the machine and reseat the chips. You don't want to open that thing up (unless you absolutely have to) so a good power strip is an easy guard against getting your computer zapped when some electrical imbalance happens.

If the power actually goes out, a consumer UPS, uninterruptible power supply, sitting between your outlet and computer can help to save your data as well as protect your computer.

A UPS is a battery backup. It powers your computer for a short time during an outage. It allows you to properly shutdown your system. As it runs, your computer has all these open little files and processes running in it. When you shut the system down, it closes all the files. The last record number and location in each little file is stored away.

Without a UPS, an outage leaves all those files standing open. The computer probably remembers the last time you accessed them, but maybe not. It takes its best guess and a message that tells you the files were not shut down properly and the system will try to recover. A UPS takes the guesswork out of shutdown and recovery.

A UPS system can cost as little as $50 or as much as $400. APC (http://apcc.com/) is one of the best-known UPS brands. Your local computer or office supply frequently has UPS systems on sale.

Software protection:

Today's computer frontier… the Internet… can be very much like the wild, Wild West of old. Cyber outlaws are out there, partner! They may be waiting to ambush you!

You should have three levels of software protection. These are anti-virus, firewall, and anti-spy ware programs.

A malicious virus attack can compromise data can be or freeze your computer. The attack can cost you a whole day. You will have to reformat, reinstall of your operating systems, application programs, and restore your data.

Viruses infiltrate from web sites, e-mails or downloaded files. Anti-virus software automatically updates itself to deal with constantly mutating infections. You will pay for these constant updates by subscription. The three leading anti-virals are McAfee VirusScan (www.mcafee.com), Symantec's Norton AntiVirus (www.symantec.com) and Trend Micro PC-cillin (www.trendmicro.com). The vendor keeps track of expirations and nags you to renew when it is time. This is almost as annoying as the viruses.

Constant Internet connections via Broadband have exacerbated another computer difficulty. Outsiders can tip toe float in over your connection to invade your data. They take your data and use it in evil ways. You need a firewall program to prevent this.

Windows XP, the operating system on most PC's, contains a basic firewall protection feature. Sometimes the Windows firewall is not enough. Commercial firewalls provide more complete protection. One well-known application recommended by CNET is ZoneAlarm (www.zonealarm.com). Others are available.

The third category of software you should have is anti-Spyware. Spyware does not pose as big a problem as viruses or intruders. When you visit

to a website, the site may implant a tracking cookie on your computer registry. Cookie? Is some twisted programmer trying to be funny?

Some cookies are good things. They allow your machine to be recognized by frequently accessed websites. Other cookies are more of the tollhouse variety. They exact a price from you by tracking your comings and goings, invading your privacy, and perhaps even selling your information. They are not usually terribly harmful, but they can lead to annoyance.

Cookies can be eliminated with available freeware applications. There are two basic free versions: Lavasoft Ad-aware (www.lavasoftusa.com/software/adaware), Spybot Search and Destroy (www.safer-networking.org.). Microsoft offers a program called Windows Defender www.microsoft.com/athome/security/spyware/default.mspx).

All spyware applications find different spy problems. You may want to download all three programs. Each program catches some spies others miss.

A word of caution: Sometimes software from different vendors doesn't work and play well with similar software from other vendors. This can cause some of those flying bytes to collide and result in the dreaded blue screen.

The collisions happen because the sadistic programmers from different companies have created their suites of programs to run on single sets of assumptions. They have expected that a line of code will react in a certain way. Mixing families of programs can mix up the assumptions between the programmers. Sick programmer senses of humor between companies are warped slightly by the companies they work for.

This can create cyber border wars. This unintended collision consequence may decide you want to use a single family of software with several kinds of protection and avoid these kinds of problems.

Microsoft is beta testing an all in one suite of programs is called OneCare Live. Included are all three categories of programs plus a backup service. According to Microsoft, this one suite of programs does everything. Contrary to rumor, OneCare Live does not make coffee or slice bread. While in beta testing, it is currently free. Expect eventually that there will be a yearly fee.

Data safety from the Mountaintop:

Your best defense against disaster is to backup your data. Implementing a backup strategy depends your level of organization and how much you value your data. Adequate data security does cost time and money.

Mid and larger sized companies hire data recovery firms such as IBM and SunGard Data Systems to store their data offsite, but the average ASPP freelance business has more affordable options.

Years ago, all we had to worry about were accounting ledgers, Rolodexes, transparencies and prints. There was no easy method for us to make copies of our important papers or get exact duplicates of our most prized transparencies. Yes we could of made photocopies of all our paperwork, but in actuality who had the time and if you ever did, where did you store all that paper? Our photographs we were able to store in archival storage medium that kept them safe from some of the

elements. What happened if there was a flood, fire, or sprinkler system was activated?

In today's world just think about what has happened over the past few years in the United States: More hurricanes than we have ever had in recorded history with Katrina the most violent storm that destroyed the Gulf Coast Region, floods, wild fires on the west coast, tornadoes hitting the Midwest, earthquakes, terrorist attacks—remember Jacque Lowe who stored all his prized negatives and images in a safety deposit box at the World Trade Center in New York. The list of possible disasters is endless.

With today's technology it is possible to replicate your data files as well as make exact duplicates, (that is you can make ***many*** exact duplicates) of all your digital images.

Analyzing the Risk and Strategy:

"You can't have 100% protection," says Reed Hoffman from Blue Pixel Inc. (www.bluepixel.com). Hoffman is Director of Education and Training and a prolific photographer. "There are two things to decide, your level of paranoia and how much money to spend," he said.

Hoffman protects his photo data when he downloads his images from his camera. Using the program "Photomechanic" (www.camerabits.com), images are automatically written to both his primary computer and a portable hard drive at the same time.

In the field, Hoffman burns DVDs of all images on his laptop. DVD's are an additional level of protection beyond computer hard drives and without the moving parts hard drive use to work their magic.

The simplest backup method is to backup your vital information on CDs, DVDs or USB memory keys. You must, however, be organized enough to remember to do it.

Consider, the vulnerabilities of the medium you are using. Not all CDs and not all DVDs are created equal. Inexpensive CDs and DVDs sometimes fail. Pay attention to where you store the disks. Proper casing that is non-abrasive and prevents scratching is vital.

Delkin (www.delkin.com) markets archival CDs and DVDs that prevent most damage susceptibilities. Light Impressions, (www.lightimpressionsdirect.com) market the archival CDs and DVDs as well as protective solutions for your discs.

Another level of protection:

The next level of protection is the portable hard drive. A 250-gigabyte hard drive is now inexpensive. Some are available for as little as $125.00. An 80-gigabyte drive is even less.

If you just can't remember to do the backup manually, you can use software designed for the purpose. Retrospect (www.dantz.com), for Mac or Windows and similar programs can automatically make backups of any folders you specify. On small networks, backups from each computer can be made to a single hard drive.

For Window users, all your preference settings and e-mails are NOT located in the My Documents folder. For Mac users, the Home folder does contain all your e-mail and settings.

(In Windows XP, to change the location of your e-mail database to the My Documents Folder: Go to C:\Documents and Settings\[my name]\Local Settings\Application Data\Microsoft\Outlook folder. Find the file Outlook.pst, drag the file into My Documents. A warning might come up that it can't find the Outlook.pst folder but once you "show" it the new location it will "remember.")

As highlighted in the books, "10 Quick Steps to Easy Backup" and "Take Control of Mac OS X Backups" a more sophisticated backup system of using **Norton Ghost** (For Windows) or **Super Duper** (Mac OS X) which can update your system regularly. After each update you will have a perfect mirror of your computer's hard drive that includes, programs, files, settings and data. If anything goes wrong with your primary machine this exact duplicate, known as a mirror, will get you up and running in no time at all.

Some backup programs make an exact image of your entire system in real time. The advantage to this technique is that it abrogates the need to spend all that time reloading your system in case of trouble. If anything goes wrong, this exact duplicate will get you up and running almost instantly.

If you have a small network, Cincinnati based "interactive consultant" Jim Cissell, Cissell Media (www.cissell.net) recommends a new device from Netgear called, Storage Central (model SC101, www.netgear.com). This device connected to your router will store and share files with all computers on your network. The storage system appears as a letter drive on your computer. As you update your files they are duplicated automatically. Additionally, you can keep certain files private as well as add storage capacity as your needs grow. .

Automatic backup system: RAID

Since many experts predict, no hard drive lasts forever, a system known as a RAID; redundant array of independent disks, provide either improved performance or a level of data protection. This system can be built into your desktop computer. RAIDs come in several varieties, but the one we are most interested in is RAID Level 1. This scheme continuously duplicates information from one hard drive to a second hard drive to insure against loss or damage. They can be any size drive as long as they are the same size, usually recommend the same model number**.** So if one drive fails you have a seamless operation with the second drive automatically taking control with all your data in place.

CNET has detailed instructions on how to configure and install a RAID. (http://reviews.cnet.com/4520-11319_7-6386531-1.html)

Online backup:

Those who do not want to deal all this backup stuff have another alternative. They are called data farms. You can store your files in several secure remote locations. On a preset schedule, the data farm accesses your computer and milks it for its data. Should anything happen to your system, you can access your data from anywhere. One drawback is that these service charge for space. You may not be able to archive huge photo collections. There are several services to choose from. C-net lists several options: Connected (www.connected.com), Xdrive (www.xdrive.com), Ibackup (www.ibackup.com), Iron Mountain

(www.ironmountaindigital.com). There are many more.

At February's PMA show, Adobe announced a partnership with Iron Mountain data farm that includes a new online photo backup service. The system is integrated with Adobe Bridge, Adobe Photoshop Elements 3.0 and 4.0, and Adobe Photoshop Album Starter Edition 3.0. The system has a of proofing and e-commerce component in conjunction with MorePhotos.com. It is expected to be operating by mid-2006. Pricing and information is available at www.adobe.com.

With all the various backup possibilities, your head must be spinning like a hard disk at 7200 RPM. I think it is all a plot formulated by those warped programmer humorists types to keep you guessing when the next catastrophe will happen.

Data safety comes down to personal responsibility. You must maintain a level of consciousness about your most precious assets, your data files. Only you can decide what your information is worth and the level of insurance you provide to your vital records.

Twisted computer humor is an honored tradition that goes back to the first computers built after World War II. It turns out that the first machines were huge, used 18,000 vacuum tubes, and broke down every 90 seconds on average. Cause of the breakdown? A moth that periodically caused a short circuit. It was the first computer bug. And the mother of all the bits, bytes, nibbles, and crashing computers to come.

Larry Levin is an ASPP national past president. Currently he spending his time as a freelance photo editor, photographer, and developing several documentary film projects. Based in Washington, DC, he is reachable by email LarryLevin@verizon.net.