Quick Lessons in Computer Maintenance,
Disaster Recovery, and Data Backup: Part 1

Introduction

The information in this article and within the series will provide a brief insight into common considerations and approaches for backing up your computer and digital photographs. If you've never thought about how your digital photos could be lost or how to recover from losing them then this article will get you started in the right direction. Maintenance tips and helpful suggestions will be given along the way. There is more information to cover than I could possibly admit to knowing myself, so I'll do my best to keep it interesting and relevant. I'd also like to invite any feedback and suggestions you have by sending them to me via email. I will gladly update the series from your feedback and suggestions as it moves along.

As photographers, specifically those of us that work with computers, it's important that we understand certain concepts when using and maintaining our computers. Most of us don't want to be computer experts; we just want the computer to work the way it should so that we can get our photo related tasks completed. I'm with you all on that one! But we can also empower ourselves by choosing to learn the fundamentals of data backup and recovery.

There are certainly thousands of creative and insightful ways of achieving the goals which this article will present. I will only be pointing out a few ways which I have been successful with during my history or those which are considered industry accepted standard. It's up to you to determine what you should do, what makes sense for you, to what extreme you go, etc. With any luck, I'll have presented you with the knowledge and a few ideas to get you started with confidence.

Note: This article, while sometimes specific to Windows operating systems, has concepts which are generic to all computers. I apologize for those of you using non Windows operating systems and hope that you're able to learn from this as well.

Terms and Concepts

Let's briefly go over some terms and concepts used throughout this article. You can skip this section and move on to the next one if you're already familiar.

1. **Data**: We could just as easily have called this "information". When talking about computers it makes more sense to refer to information as data. Data is a generic title used to describe many things found on a computer including files that contain emails, bookmarks, and digital photographs. Data also includes less familiar things like "File Allocation Tables", and "Master Boot Records". These last two are data stored on your hard drive that aren't accessible in the same way you would open files normally but they exist nonetheless.
2. **Data Loss**: Any time data changes or is deleted you have the potential for data loss. Sending a file to the "Recycle Bin" is a potential for data loss. Your hard drive going up in smoke is a potential for data loss. Data loss is permanent once you've decided that the data can no longer be recovered (or all recovery methods have been exhausted.)
3. **Data Recovery**: Data recovery is the name given to a process that restores lost data. The windows recycle bin can be used as a simplified example of data recovery. If you sent a file to the recycle bin (an example of potential data loss) and later restore the file from the recycle bin, then you have just recovered data that was potentially lost.
4. **Data Integrity**: Data integrity is the expected "potential" and "possibility" for data to be lost. It's easiest to understand this concept when we're talking about storage mediums. Some storage mediums are more stable than others. The data that is on medium specified as lasting 20 years would have more potential data integrity than the same data on a medium specified as lasting only 5 years.
5. **Storage Medium**: A physical device upon which data is ultimately stored or "written to". Examples include hard drive, CD-ROM, DVD, compact-flash, tape, floppy, etc.
6. **System Performance**: I think most of us understand what this means. If you're talking about how quickly your hard drive accesses data you're probably talking about system performance related items. If you're worried about "How fast?" or "How well…?" it's probably performance you're talking about.
7. **System Maintenance**: By maintenance I mean anything that is done to keep the system performing well and to prevent degradation of system performance and data loss.
8. **Disaster Recovery**: Unlike losing a single file like a digital photograph, disasters happen when your whole hard drive is

permanently damaged or a virus deletes every file on your system so that it no longer boots (turns on). Basically, think of anything that causes your computer to be unusable and/or destroyed. If someone came into your home and stole your computer, that would be another good example of a disaster. The process used to recover from these kinds of disasters is what we call disaster recovery.

9. **Data Backup**: Data backup, in simplest terms, means making a copy of data so that it exists in multiple locations simultaneously. You'll often hear terms like "redundant data backup" or "triple redundant" which basically means having more than one copy of the data.

No data storage mechanism is permanent

When I say "storage mechanism", I just mean storage tools, storage processes, storage mediums, or some combination of those. There are vast amounts of information available which detail the good and bad about the various popular storage mediums. What we're worried about here is data integrity.

Did you know that it's not uncommon for brand new hard drives to fail only a few days after using? Did you know that direct sunlight can cause serious data integrity issues with CD-ROMs and DVD's by quickly eroding their lifetime? Did you know that heat and humidity have an impact on the useful duration of most if not all types of storage media?

So what does it mean to us then when a manufacturer specifies that a CD-ROM has a lifetime of 20 years? 100 years? We need to translate what they're saying into what it truly means: They did controlled testing in a controlled environment. And in that environment they made measurements. The results of those measurements allowed them to specify that it'll maintain data integrity for 20 years. I'm severely trivializing the whole process, but what I've said is generally true. They obviously didn't test the medium for 20 years but that's beside the point anyway.

Instead of getting into the nitty-gritty of all of this and using fancy graphs and charts ask yourself the following types of "what if?" questions:

1. "What if my media got wet?"
2. "What if my media were exposed to very high temperatures (fire for example)?"
3. "What if I leave my media in direct sunlight?"
4. "What if my media were physically scratched? Dropped?"
5. "What if X years from now you can no longer get the hardware to read or write the medium?"

I think you get the idea. All of these things cause the 20 year specification to be meaningless in most applications. Lifetime and longevity ratings are extremely useful when deciding what medium to store your data on. They are so useful in fact that if you're not using that information as part of your decision factors, then you might not have as safe a solution as you thought. Unfortunately, long lifetime and high longevity aren't the final word.

Common sense combined with a little extra knowledge and additional precautions go a long way into keeping your data "alive" and healthy:

1. Take notice of the manufacturers recommendations where they describe the recommended storage conditions. Most mention to put in a dry, low humidity, low temperature environment with no direct sunlight. Follow their recommendations.
2. If you require constant access to the storage medium, choose a medium that is less prone to damage during transfer or by direct contact. CD-ROMS are prone to scratching while tape cartridges are fully protected by their case. Optical media exists that is completely enclosed in a hard protective case (much like a zip disk is enclosed). Take these kinds of things into account.
3. If you require CD-ROM jewel cases you may have noticed that they make completely clear cases, black cases, and every color and tone in-between. Wouldn't it make more sense to buy the black ones because they block the sunlight from reaching the CD while it's in the case? Of course it does! Whether it matters or not probably depends on where you store them but it's another example of something trivial that could make the difference.

So what else can I do to help with data longevity and to keep my data alive and healthy?

You probably noticed the "What if?" question above concerning the hardware being available in the future to read the data. This is a real problem with numerous examples today where it's already happened or is happening. Fortunately, there is a very easy solution to the problem! Make it a habit to upgrade your data backups to whatever the newest technology is that suits your needs at the time. For example, if you've been backing up on CD-ROM now might be a good time to switch to DVD. Copy all of your old CD's

onto DVD. A year from now, copy your DVD's over to the next newest standard or format. Now simply "Rinse and Repeat" every year or two.

What other issues do I need to be concerned with

As photographers, we have a special interest in keeping our photographs available to others. For many of us it's important that others can access our photographs should we pass away unexpectedly. This is a serious issue with no quick and easy answers unfortunately. Traditional photography allowed all of the photographs and negatives to be held in your hands and stored in boxes. We didn't need computers to look at the photographs or make copies from negatives.

The only recommendation I can give is that you print out all of the photographs now that you want future or current generations to have. Use the same archival standards with your photographic prints as you do their digital counterparts. You might also provide written instructions describing how your photographs are stored digitally and how to get them (what software to use, where the backups are located, etc). These instructions could be written for someone specific in your family or could be written for a professional service. Either way, it might be a good idea to have an actual person as a backup for your own person. I realize this sounds silly, but if you think of yourself and your knowledge as being the "data" then what you're looking for is a backup plan for yourself. Coincidentally, this is the area where the longevity of the medium becomes much more important (post death that is).

Personally, I don't need to deal with this kind of problem because I'm going to live forever…….Sound silly? It should. It's just hard for us to consider these things in the course of everything else we're worrying about. Remind yourself every now and then that you're not going to be here forever and you'll likely make better decisions. Don't worry about your friends and fellow photographers making fun of you.

Never rely on data recovery mechanisms or processes

Have you ever sent something to the Windows recycle bin knowing that you could restore it later in case you still needed it? Do you habitually empty the recycle bin without thinking about it (I know I do)? Have you ever answered yes to these last few questions only to find out that you did in fact need that file? Too late now isn't it?

No disaster recovery or restoration process is perfect. You could spend no money or a million dollars on disaster recovery tools and still lose your data because of that one little event you never thought of.

Use the recycle bin example. If you're relying on it to protect you from permanently deleting your files, there are many things that could go wrong including:

1. You could do like I sometimes do and empty the contents unconsciously before you actually intended to.
2. You might assume that certain programs send deleted files to the recycle bin only to learn that they don't use it at all and the file goes straight to "La-La-Land".
3. Files in the recycle bin might have an expiration date that you weren't aware of and the recycle in removes then automatically after that date.
4. The recycle bin might be full so it's no longer retaining all the files sent to it.

"But wait!" you cry in protest. "That's why I use that XYZ software that can undelete files even after the recycle bin has been emptied and even if it never went to the recycle bin to begin with!" Good point and a clever one indeed. It's definitely a smart thing to do if you're using that kind of software. The problem, however, is that while these software packages are excellent tools in restoring deleted or lost files, there is no guarantee that the files will ALWAYS be retrievable. Without going into boring details of Windows based file systems it's important to understand a few basic facts about this type of data recovery software tool:

1. There is no guarantee that each and every lost file can be recovered.
2. Don't assume that it can recover every byte of the file, byte for byte.
3. The longer you wait to do the recovery the less your chances of recovery are likely to be.
4. The more activity you do on your computer before trying to recover the less your chances of recovery are likely to be.
5. The larger the size of the file to be recovered is, the lower your chances of recovering it become.

It's entirely possible (and quite likely) that rebooting your computer is enough to permanently impact the ability for the data to be recovered. The absolute best thing you can do once you realize you've lost data is to stop and do nothing. Take the time to think about what you should do or ask an expert if you need help.

If you're thinking ahead, you may already have figured out that I'm presenting you with something of a riddle or paradox. How can I have a reliable data backup and recovery system without relying on the system itself? The answer to this riddle unfortunately is that you can't. The good news is that there are tricks to help combat this problem. For example; introducing redundancy allows for one or more failures in your process before data is permanently lost. Redundancy is the best answer to the problem this riddle is trying to address. Instead of relying on one system, rely on many and hope that they don't all fail at the same time. The more redundancy you have in the system, the better your odds are that you'll have a way to recover the data. How far you go is a matter of choice. Does your life or livelihood depend on this data or is it just convenient to have around? Will clients sue you if you lose their information or is the information for your needs only?

Paranoia is good

By now you may be thinking that I'm overly paranoid or sensitive about the subject of data loss. Those that are thinking this are probably the ones that have been fortunate enough to never have run into the problem before. Sometimes the hardest lessons to learn in life are learned in the hardest of ways. I'm not trying to suggest that everyone should have their data backed up. Its importance should always be evaluated on a case by case basis and the best person to determine that is you.

No one should live their lives feeling paranoid. I agree with that statement. That's exactly the reason why we should have a good process in place to keep our data safe. A process that allows us to "set it and forget it" would allow us to live with much less paranoia than a process where we have doubts about whether it's good enough or if it'll work as planned.

There are (or should be) limits to all madness of course. Exercise of a little paranoia is both healthy and human. Your hard work in coming up with a good system will have a bigger payoff than you may realize.

What's coming next?

In the next issue of this series, we'll begin looking at a few of the common types of software tools used for backing up data. We'll learn how they each work as well as their advantages and disadvantages.

Editor's Note - Trevor Ash is employed by a large test and measurement company as a Software Quality Assurance Engineer. Visit Trevor's website at www.persistinglight.com.

TA - NPN 0830

Comments on this article? Send them to the editor.