

Disaster Recovery: It's All In The Planning

By Bill Hely

The term “disaster recovery” means different things to different people. Even confined to events that affect the usability of computers in the conduct of business, a “disaster” can have a wide range of meanings, and “recovery” can vary quite considerably in scope. In this article I’m going to restrict the meaning of “disaster” to mean data loss.

We will not concern ourselves with how the data may have been lost, other than to reflect briefly on the fact that events that can cause data loss are many and occur frequently. They include...

- fire
- flood
- equipment failure
- earthquake
- electrical surge
- user error
- theft
- vandalism
- vindictive acts

...to name just nine of many possibilities.

And that’s not even considering the most frequent cause: just plain bad luck—things over which you have no control at all, such as a hard drive crash or power failure at just the wrong moment. Similarly, we’ll use only a narrow definition of “recovery”, as in “getting back data that was lost”.

Beyond that, smart entrepreneurs will have at least a rudimentary *Disaster Recovery Plan* in place. The DRP will include information on where to quickly source replacement computers (temporary hire, for example) and all the other things that will need to be done to get a business up and running again very quickly after a catastrophic event.

Under certain policies, insurers may require that a Disaster Recovery Plan be submitted for approval before cover is granted. For information on DRPs—also called Business Continuity Plans—perform a web search; there’s a lot of information out there on the topic. Thinking about such things now may save your business in the future.

In practice, a diverse mix of methods is used to take copies of important data, ranging from doing nothing (a disturbingly large number) to complex, expensive and dedicated network-attached storage devices.

Methods in common use include burning to CD, copying to floppy (rare these days due to large file sizes), copying to another PC on a network, storing to the near-obsolete ZIP, JAZ or LS-120 drives, detachable USB storage devices, and so on.

And of course the venerable Tape Backup Unit (TBU). There are dozens of different tape formats, the most common being the 4 millimeter Digital Audio Tape (DAT). Regardless of tape format or drive type, this method is usually just referred to generically as “tape backup”, with only the IT professional concerned with specifications.

But no matter which method or storage media you use, backing up critical data is a largely pointless exercise if that backup remains in the computer, in the office or even in the building. Considering only the nine types of disaster I listed in the bullet points above, at least six of those can also render your backups useless, along with the original data, if the backup is not taken completely off-site.

Now before you start to anticipate where I’m going here: No, I’m not about to just repeat the admonition you have doubtless heard *ad nauseam*—to take your backups off-site each night. If you haven’t been doing that up to now, then my harping is unlikely to make you change your ways.

Disaster Recovery: It's All In The Planning

And even if you have been taking your backup's off-site, how effectively have you been doing it? Will you be taking yesterday's backup with you when you leave today, and leaving today's backup running?

Hey ... I understand. Who wants to hang around after work every day for an extra hour or more waiting for a backup to run? And unless you are using some automated method with fast, large capacity removable media, it could take much longer, depending on the size of your operation.

If you are manually backing up to some other media — say CD/DVD or ZIP drive — then you have even more work to do and no guarantee that you will be getting every important file off every computer.

Another thing to consider: just how certain are you that the data you are copying to a backup media is “good”? When was the last time you performed a test “restore” from your backups to ensure that all was as it should be? I can tell you from long experience how often the average person does a test restore.

Never!

Your main concerns should be:

- Have you got a copy of all the files you should have?
- Have you really got the very latest version of each of those files?
- Was the data transferred from hard disk to storage media without error?
- Is the integrity of the storage media 100%? It only takes a scratch on a CD or a kink in a tape to render a lot of data unreadable and thus unrecoverable.

Finally, the catch that few people ever think about until too late...

Let's say you have an important file that gets updated periodically, a spreadsheet for example. Let's also assume that today someone accidentally deleted some cells or made a significant error in that file—an error that was not caught at the time. The file is saved and you take a backup. This goes on for a few days—edit, save, backup—before the problem is noticed.

What now? Of how much use will your backup be? Even if you are making redundant copies, how far back can you go to recover a pre-error copy of the file? For most small businesses the answer will be from zero to a couple of days at most.

OK, I could go on and on with examples of the problems you can face even if you are making backups, but it's time for some answers.

Look, this is the Internet age, right? If it wasn't for the Internet you wouldn't be reading this, so I know you are connected. Further, if you are in business you probably have a broadband connection. The Internet connects you to “the world”.

Look at it another way: In backup terms, the Internet connects you to off-site servers. With the right accounts and services it connects you to **off-site storage**. And it's those special services (and they are certainly available to you) that will make all the difference.

In my small office I have two tape backup drives, a couple of USB drives, several CD burners, floppy and LS-120 drives, external hard drives and networked computers. That's a lot more storage options than many small businesses would have.

Disaster Recovery: It's All In The Planning

For long-term storage of files that I may never need again, but which I have to keep anyway (e.g. accounting records), I burn to CD or DVD. For everything else I back-up to "the Internet".

That's right. I've got tape drives and tape backup programs and I no longer use any of them.

My backup is scheduled to take place in the evening when the office is empty. That backup is 100% automatic and requires no initiation from me. None at all. No swapping tapes, no inserting CDs, no anything else. The system I have in place automatically and without any prompting backs up any file that is new or that has changed since the last backup. Plus, the backup system keeps the ten most recent versions of every file backed up during the last 90 days.

And I do all this with no capital outlay, no extra hardware, no media to deteriorate and need replacing, no need to "remember" to take some action.

Online backup services are not all that new, but finding one that is extremely reliable, very easy to use, very affordable (even for an individual home user), and requires no term contracts is not at all easy.

At the end of this article I'll give you a link to the free software that makes all this possible, but don't jump ahead and anticipate. First a brief description of how the program works is important.

No need to take notes, memorise or even thoroughly understand the following points. Just want to give you an idea of just how easy it is to implement for yourself the sort of safety I enjoy. The steps are:

1. Install the free software;
2. Open the software's Backup View Tab, then select "Explore to pick files" on the left of screen.
3. Use the Windows Explorer-like interface to mark the files/folders you want to include in your backup schedule. You only need to do this once, unless you change your mind at some later date.
4. From the Menu bar select *Options* → *Backup schedule* and set a time when the backup will run automatically.

That's all there is to it! Even new files added in the future to folders that you selected for backup (e.g. My Documents) will be backed up without your having to include them. As will, of course, any existing files that later change.

Now you just get on with your life and leave the program and the remote service to "do their thing". Each morning (I prefer my backups to run at night when I'm not using the computer) the main window of the backup program will provide a brief summary of the backup and report any problems (very rare).

Only new files and the changed parts of files previously backed up are transmitted to the data center, and the data to be backed up is compressed for the transmission, so backups are fast and efficient. Also, your precious data is securely encrypted before transmission and is stored at the data center in its encrypted form. Even the data center technicians can't make sense of it.

If ever disaster strikes your PC, recovery of your files is just as easy, and they can be recovered from any computer anywhere in the world, so long as you have the correct access codes.

Disaster Recovery: It's All In The Planning

If you have any care for your data at all you really should try this. The software is free and the service is very affordable. There's a 15-day free trial of the service, after which you are invoiced monthly, quarterly or annually, as you prefer, and you can quit at any time without notice. This is the very best way for individuals and small businesses to ensure reliable recovery of data with minimum cost, minimum risk and minimum effort.

Oh, and in case you're wondering what happens if the data storage center itself suffers a catastrophe ... each day the data you have stored at the center replicates itself to another data center in an entirely different geographical location. These data centers are extremely high security locations—armed guards, gas fire control, standby generators, the works. These same data centers are used by some of the worlds biggest financial institutions, so no effort is spared on security and reliability.

In under half-an-hour you can put backup problems behind you forever. Or ... you can wait for Mr. Murphy to come calling. You already know he only visits at the worst possible time.

As an extra safeguard I also use the Carbonite service, though in almost all respects it is inferior to the previous method. The biggest drawback is that it can take days (even weeks!) to process your initial backup.

However, in the event of an irrecoverable disk crash, it's just possible that you may be able to retrieve some data through Carbonite that was new or changed since your last main backup.

Fact is, the two methods are best used together.

Download the installation file you'll need for your 15-day free backup trial from here:

<http://www.DataSafetyCenter.com>

Learn more about the Carbonite service here:

<http://HackersNightmare.com/Carbonite>

And do it today, before something happens. After is way too late.

-oOOo-

Bill Hely is a technologist, consultant and author living in Brisbane, Australia. For most of the last two decades his professional focus has been on advising and supporting small business operators in Information Technology and Office Productivity. He is the author of several books on technology for the business operator, including the Bible of Internet and computer security *The Hacker's Nightmare*™.

To comment on this article please use the "Support" link at the bottom of the <http://HackersNightmare.com> main page.

Comments, suggestions, expressions of appreciation
— and especially testimonials —
are most welcome.