A laptop, a coffee, and disaster recovery

Why you should have an effective backup strategy

John Locke

Last week, my laptop died a sudden spectacular death-by-drowning, as a full cup of coffee poured into its keyboard. It emitted a pop sound, and the screen and the power shut off.

What would your reaction be? Mine was to immediately unplug the power cord and remove the battery. Then I took it over to the sink and poured out the coffee. Remembering tales of people flushing keyboards with water, I ran some fresh water over the keys and then set to work. I removed the keyboard, the palm rest, a few of the inner cards, and let it sit without power for several hours. Apparently, not long enough.

Later that day, anxious to find out whether it was really dead or just comatose, I plugged it back in, crossed my fingers, and pressed the power button. The power light came on, I heard the fan start, and for a second or two, I was hopeful. But then… another pop, and it was dead. No further cleaning, drying, or care could resuscitate it over the next few days, so it's currently back at the IBM factory going through open-heart surgery, if not a total replacement.

What can go wrong?

Obviously, if I didn't have a good backup of my data, such an event could have been catastrophic to my business. As it was, the loss of my laptop was merely an expensive hassle. Actual events such as this one can provide a good reality check for your disaster recovery strategies.

Many things can happen that have a similarly disasterous effect. Being prepared for disasters can make life easier if the event actually occurs. Let's take a quick look at some possible computer disasters:

- Coffee fries the laptop.
- A service technician copies sensitive data from your computer.
- Your laptop is stolen.
- Your data is erased by a malfunctioning airport X-ray machine.
- Your house burns down.
- Your PDA is stolen.
- A virus infects your files, and your recent backups.

Which of these disasters could make you go out of business? Or subject you to identity theft? Or to a lawsuit from your customers for leaking their information?

Many things can happen that have a similarly disasterous effect. Being prepared for disasters can make life easier if the event actually occurs

Several issues come into play here, and you need to consider all of them:

1. Loss of use of your equipment.
2. Compromise of sensitive data.

3. Loss of data, including corrupt backups, deleted files, or important files you change accidentally.
4. The overall risk of any of these events.

These are some of the considerations to be made when planning your disaster recovery strategy, and I'll get into more detail in future issues.

The best backup system is one you don't have to think about at all. Ideally, your laptop or workstation should have no data that's not also stored somewhere else

How do I back up my data?

There are several approaches to doing backups. It used to be that most places would get a tape-drive and put entire system backups on a schedule to run overnight. Tapes aren't always reliable, though, and it can be very difficult to retrieve individual files.

These days there are a lot more options. Writable CDs and DVDs provide a cheap way to create permanent backups, and create historical archives. USB thumb drives make for a simple way of instantly making a copy of important files. Large hard drives are cheap to buy, and when installed in an external drive enclosure or removable casing, become the most economical way to back up large sets of data.

If you have a Local Area Network (LAN), you can backup important files by simply copying them to other computers. If you're in an office environment, I highly recommend having a server, and concentrating your backup efforts onto the server instead of individual workstations.

The best backup system is one you don't have to think about at all. Ideally, your laptop or workstation should have no data that's not also stored somewhere else. We're all human afterall and the more work it is to do a backup, the less likely you are to have done one when you need it. So how did I do, when my laptop died?

Painful self-analysis

I probably rely on my laptop for a wider variety of data than most people. An important part of your backup strategy is identifying what data needs to be backed up, how often, and where. Here's a list of what was on my computer:

- Email
- Contact addresses
- Calendar/Schedule
- Password database
- Sensitive customer files
- Sensitive business data
- Finances
- Non-sensitive customer files
- Non-sensitive business documents
- Prototype databases for web application projects
- Prototype web applications under development
- The operating system and application software
- Configuration details about the machine itself

This list is probably a lot longer than yours, but it covers most of the different types of data used by the majority of small businesses, and may include a couple things you haven't thought about. So, how did I go with my disaster recovery strategy:

Email

A perfect score. My email system uses IMAP, which keeps all mail on the server. Every single email in my mailbox is intact on the server, and immediately available from any other computer.

Contact addresses

Not so good. My contact addresses are currently stored in Evolution, my main email software. I periodically back up by synchronizing to my Palm, but I had been having problems with the synchronization, so I hadn't done that for a couple weeks. I could have lost the last two weeks of any changes to my address book.

Calendar and Schedules

Ouch! My strategy was completely inadequate in this area. Evolution has great calendaring capabilities and I have several different calendars set up in Evolution, each for a particular type of work. My meeting calendar gets synchronized to my Palm PDA. My social and meeting calendars are merged to publish free/busy information so others can schedule meetings with me. I then keep several other calendars to block out time for different tasks: billing, taxes, security updates, client projects, and articles. In Evolution I can easily show or hide different calendars, and see when

I'm available for a meeting. But the downside is, these calendars are all stored only on my desktop. Evolution does not yet support storing calendars on a server - though you can read remote calendars. Aside from the meeting calendar, the remainder of my tasks and work schedule would have been completely lost.

These types of events always serve as a wakeup call, highlighting areas for improvement

Password database

Okay. It's there, a backed up copy from my PDA. It's also encrypted, though the encryption is not as strong as other encryption methods. At least it'd take substantial effort to crack, and I can trust IBM, with its reputation, not to mess with it.

Sensitive customer and business files

Good. Not only are all my customer files in a server-based document repository, available for instant access from any other computer, but the copies on my laptop are on a strongly encrypted partition. My clients and I have nothing to worry about when the hard drive goes into the service depot: the encryption method used is the Advanced Encryption Standard (AES), which is the US Government standard for strong encryption and currently has no known flaws.

Finances

Super! My finances aren't even stored on this machine, even though it's my primary workstation. I use a web-based application, with an encrypted connection. My business finances never leave my server, and the server is backed up nightly.

Non-sensitive customer files, prototype web applications

Good. Again, all customer files are stored in a document repository, and I work on a local copy. Whenever I'm done for the day, I check these files back into the server. I could have lost a few paragraphs, written in a new proposal that morning; but in this case, there was no catastrophic loss.

Non-sensitive business documents

Poor. I had a lot of marketing material in my computer that was not backed up anywhere else. Chunks of text getting prepared for the web site, a couple of time and mileage tracking spreadsheets, a few other assorted files were not properly added to my document repository. The mileage tracking spreadsheet in particular would have been a tough loss.

Prototype databases

OK. If you're not a developer of some kind, you probably don't have any databases running on your laptop. I have three: MySQL, PostgreSQL, and Oracle. It's one of the main reasons I got a new laptop this year - to get the performance I need to handle the types of development I'm doing. Databases often can't be backed up as files, especially when they're running. But there's nothing in the databases on my laptop beyond sample data, and the structure of each database is regularly exported to a file and added to my document repository. The document repository itself is a type of database that entails special backup procedures, but that's not on my laptop, so that's a story for another day.

While I had most of my critical data automatically backed up, there was a significant hassle involved in losing the data stored only on the laptop

Operating System and software

Just fine. Many people back up the entire hard drive, just because that's what they think is necessary. I never back up the operating system or installed programs. In the Linux world, it's almost always better to install the newest version of any software - catastrophic loss of a computer is just a great opportunity to upgrade. In the Windows world, you tend to need to periodically reinstall the entire operating system periodically anyway - especially the way recent spyware and viruses have infiltrated so many machines. Much better to start fresh and install the programs you need when you need them, either from new versions or directly from the installation CDs that you have in the bottom of that drawer.

System configuration

Total loss. On one hand, I try to keep the system configuration as close to the default as possible. But I had done a fair amount of custom configuration on this laptop to support things like the infrared port, the modem, and the wireless card, as these things don't always work reliably out of the box in Linux. I have notes around here somewhere, but didn't put them in a central place and some of the stacks

of paper around here qualify as their own disaster needing recovery.

Result: needs improvement

While I had most of my critical data automatically backed up, there was a significant hassle involved in losing the data stored only on the laptop. In particular, I need to improve my contact, calendar, and a few less critical business documents. I also need better documentation of my system configuration. This would help me get this laptop back up, and running much more quickly.

Fortunately, I didn't lose a thing. I went down to my local electronics store and bought a little drive enclosure for a laptop hard drive, plugged it in and recovered everything on the drive, including the things I didn't have well backed up. All the same, these types of events always serve as a wakeup call, highlighting areas for improvement. Top of my list, based solely on the value of the data, is getting a better system in place for storing my contacts.

How would you fare if you lost your primary computer?

If you don't feel confident in your current backup strategy, we at Freelock Computing would be happy to help you figure out a better plan. Next month I'll look at options for encrypting sensitive documents. It's easier than you may think.

Copyright information

About the author

John Locke is the author of the book *Open Source Solutions for Small Business Problems.* He provides technology, strategy and free software implementations for small and growing businesses in the Pacific Northwest through his business, Freelock Computing (`http://freelock.com`).