

Data Preservation

You're as secure as your data.

Data. In today's world, more and more companies see that their primary source of revenue is information – data. Creating, editing, analyzing, auditing, updating, maintaining, managing... the list goes on and continues to grow. As we continue to move toward a world without paper, we become increasingly reliant on disaster prevention, data preservation and recovery. A company can literally live or die based on safety and security of their electronically stored information.

Easy come easy go.

Easy data access and speedy data transfer are principals of productivity in our information age. Of course *data that can so quickly and easily be accessed can just as quickly and easily be damaged, deleted, and destroyed*. All it takes is one unfortunate event be it accidental or deliberate, and all that data disappears in an instant, along with all of the billable hours, days, weeks, and even years that went into its creation.

The cost and the odds of survival.

In [Data Loss... Can Your Company Survive? \(Most Do Not\)](#) Harald Anderson writes:

Data loss can cost your company uncountable hours in lost productivity and revenue. In addition to the direct loss of a potentially unlimited amount of data (and the payroll hours that it took to generate that data) your company's business and potential to generate revenue can also be crippled by even the most minimal of data-destroying meltdowns.

*Imagine the loss of productivity that would occur if your accounting department suffered the loss of all of their files. In fact, 20 megabytes of accounting data takes 21 days and costs \$19,000 to reproduce. **Among companies who lose data in a disaster, 50% never re-open and 90% are out of business within two years!***¹

All your eggs in one basket.

When it comes to preserving your data, redundant local hardware is an obvious and essential first step. The thing to remember about redundant local hardware is that all of the redundant hardware at any one location is at essentially the same risk, be it from theft, fire, flooding, electrical spikes, or even unhappy employees. A colleague recently told me of a firm he worked with, that had their entire RAID array go down. Now this is an extremely rare occurrence, and that may be the reason that they had chosen to forgo any off-site backup. The good news is that they were able to recover all of their data by sending their drives to a data recovery specialist ("clean room"). The bad news is that it cost them \$5000.

¹ Anderson, Harald. [Data Loss... Can Your Company Survive. \(Most Do Not\)](#). Retrieved on 2007-07-30.

Old school.

The next step for many companies is maintaining hardware and/or media that is routinely (more or less) taken to and from the business. While this does offer a bit more protection from data loss by physically taking it offsite, it carries many of the same risks as your local hardware. The risk of theft can be greater, as the drive or media is often kept in a less than secure location (like the trunk, or even the back seat of an employee's car) and most often this data is unencrypted and thus free for the taking in addition to the hardware.

What's a week worth to you?

Even with redundant on-site and off-site (to and fro) hardware back-up, considerable data (time) can be lost both deliberately and accidentally. Due to the logistic concerns and labor-intensiveness involved in transporting hardware or media to and from work every day, many companies do this only on a weekly or even longer basis. A local hardware failure in the weekly scenario might instantly cost you a week's worth of data along with the time and money you spent to have it created.

The Human Factor.

Further complications to both local and off-site redundant hardware can come in the form of forgetfulness to take the data off-site and/or keep the data regularly backed up in the first place. While the local back up process may or may not be automated, the human component is always a factor in the physical removal and replacement of the hardware or media.

Keep it simple.

An ever growing number of companies are preserving their data through the use of online secure backup and storage providers. This eliminates a great deal of the risk by removing most of the human factor. The best providers simplify the process with automatic backup that encrypts and sends the data out the moment it is saved to the drive. Nothing to remember and nothing to forget, not even a schedule to set-up – totally automatic, and largely fool-proof. Another good idea is to find a provider that only charges for what you use. Some providers use a package model that leaves you paying for large blocks of storage space - more than you really need, so look for one that only charges for what you actually store.

Caveat emptor.

A word of warning: the market for remote storage and backup has exploded over the last few years. The good news is that caused a significant reduction in price across the board. The bad news is that many of the low-cost providers focus only on price, and may not have a sound business model (they're not going to be here long), and/or sound security practices (and neither is your data). Sound advice: Make sure that the provider you choose has been around long enough to be proven, and provides documentation of their security practices.