



Many companies fail to fully safeguard all of their critical computer files. Financial journals, payroll records, inventory databases, email correspondence, customer lists and marketing materials are some of the most critical files on your computer. For the midsized companies, even SQL databases or Microsoft Exchange Data are often overlooked.

If this information was suddenly lost, stolen, or somehow compromised, could your business survive? If so, at what cost? Most of today's PCs come with a means of backing up critical data (mostly desktops). It could be a floppy disk, zip drive, tape drive or CD/DVD writer. Even those systems with no internal backup hardware will support external Firewire or USB storage devices.

The investment required to purchase a backup device these days is relatively low. So, when a user fails to perform backups, it is rarely due to lack of a computer storage device.

The real issue is that it takes time and specific knowledge to identify the critical data which must be archived - and - expertise to implement and test a regular backup process. Very often it is determined after a loss that the critical data wasn't even included in the backup routine. Only with proper preparation and testing can one be truly confident of complete data recovery in the event of a problem.

Larger companies have dedicated Information Technology (IT) staff assigned to perform backups. Smaller companies generally do not. For the small percentage of small companies that are fortunate enough to have an IT person, it is typical for them to be over-committed and consistently in "fire-fighter" mode...and too busy to be the backup coordinator. Sadly, the very last thing on the daily to-do list of most small business owners is to perform a backup. And, as we all know, busy people frequently don't reach the end of their daily list of tasks!

If it takes a staff member just 15 minutes per day to oversee the backup process, and that staff member costs \$20 per hour, you are probably spending over \$100 per month in direct labor alone - just monitoring the backups. That does not include the cost to maintain the equipment or to purchase initial or replacement media (tapes, CDs, etc.)

There are many questions you could ask yourself about data backups. These might include: If the employee responsible for backups goes on vacation or leaves the company, is another employee standing by ready to perform regular backups? Are backups being stored offsite in the hot trunk of car, melting away?

Has anybody ever tried to restore data from a backup archive? Business owners frequently don't realize that most computer backups are not password protected or encrypted. A disgruntled employee or competitor that gets a hold of one of your backups now has a list of all your customers and all your important financial information. To many, this is very scary!

Computers are very fragile electronic devices and threats to them are everywhere. In fact, lack of proper computer backups has led to an entire premium-priced service industry dedicated to

retrieving data from failed computer disks. Per incident recovery fees of well over \$1,500 are common.

Something as simple as a spilled cup of coffee could completely destroy a computer rendering volumes of data unusable. A surge on the power line, a disk drive malfunction, an accidental format command, security vulnerability, software bug, stolen computer, a virus or even a simple human error could all cause irrecoverable damage to vital computer files. As we have seen recently, physical threats such as fire and flood, although infrequent, cannot be ignored. The fact of the matter is that eventually all computers fail. They are electromechanical devices with moving parts. These parts have a finite service life and there is no way to tell exactly when they will fail. It is always amazing how after an unexpected computer failure, no amount of money is too much to recover yesterday's critical data. Yet, often, business managers are reluctant to pay the relatively small cost (\$1 or \$2 per day) it takes to put a basic offsite backup solution in place.

So, what about your backups? The Level2 Offsite Backup Service is a secure and cost-effective solution for many small-to-mid sized businesses that do not have the staff time or knowledge required to properly perform their own daily backups. Our HIPAA compliant solution could just save your business!