



Dr.Backup™
online backup service



Are You Safeguarding Your Data?

Many businesses 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.

If this information was suddenly gone, could your business survive?

Virtually all PCs come with the basic software needed to back up critical data to external media. So, whether you choose to use CD/DVD, thumb drive, portable disk – or even a tape drive -- the media costs are generally affordable.

So, when a small business fails to protect critical data by performing backups, it is rarely due to a lack of resources.

It takes time and effort to keep track of critical computer data that regularly changes and hence must be archived. Organizational discipline is also required to ensure a backup process occurs on a regular basis.

Still, even if backups are performed, they must be tested to be certain that a data recovery is possible in the event of a mishap.

Larger companies have dedicated Information Technology (IT) staff assigned to perform backups. Smaller companies do not, and even if they did, this person would typically be over-committed and consistently in fire-fighting mode...too “consumed” to do routine backups.

Sadly, the very last thing on the daily to-do list of most small business owners is performing a backup. And, as we all know, busy people frequently don't reach the end of their daily list!



If it takes a staff member just 15 minutes per day to oversee the team backups, and that staff member costs \$20 per hour, **your business is probably already spending over \$100 per month in direct labor** - just monitoring the backups.

But what happens 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?

Are you confident that files can be restored from the backups performed by the receptionist?

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 your backup media now has a list of all your customers and all your important financial information.

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 \$5,000** are common on servers.

Something as simple as a spilled cup of coffee could completely destroy a desktop computer rendering volumes of data unusable. A surge on the power line, disk drive malfunction, accidental format command, security vulnerability, software bug, stolen computer, a nasty virus or even a simple human error could all cause irrecoverable damage to vital computer files. As we see on television, **physical threats such as fire and flood**, although infrequent, cannot be ignored.

Fact of the matter is that eventually all computers fail. They are electronic 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 (\$2 or \$3 per day)** it takes to put a basic offsite backup solution in place.

* * *

So, what about your backups? The **Dr.Backup** online 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-compatible solution could just save your business!