

A Practical Guide to Data Protection for Small Businesses

By Jim Walker

NOTE: This article was written by Jim Walker originally for SNW Online.

Pam Landa is one of the lucky ones. As a successful freelance photographer in the San Diego area, she focused on her strengths in photography. As a small business owner, she knew enough to seek expert advice in areas that were not her strengths, such as personal computer technology. Soon after a friend recommended that she implement a structured system for backing up her business data, a computer virus shut down her system. Fortunately, Pam had arranged for a remote backup service to backup up her critical business files, which saved her from a business disaster.

As Pam puts it, "I'm not sure of the exact dollar value of my data, but I was glad to be able to recover all of my e-mail folders with various discussion threads, all of my orders in process, the professional technical tips I've picked up over the years, accounting data and more."

With our increasing reliance on computer technology, the amount and value of electronic data is also increasing. Add to this our reliance on e-mail, as well as legal compliance issues for medical and public companies, and you find that often the company database is one of the most valuable company assets.

In spite of the high visibility of hurricanes, fires and other natural disasters, the greatest dangers to small businesses are technology drive threats. Small business is particularly vulnerable because there is seldom an IT specialist inhouse. Best practices for virus protection and data backup often take a backseat to more urgent issues. The consequences of data loss from these threats, however, can be significant. Loss of data will cause an interruption of business, often times leading to a loss of intellectual capital. In addition, a compromise of client information can mean a loss of trust and legal liability.

Once a data disaster has occurred, the cost of recovering the data or attempting to recover it can be very high. Forensic analysis of a hard drive can run up well over \$3,000 with no guarantee of success.

Traditional approaches to formal backup include using external hard drives, tapes and weekly copies to a CD or DVD, which are then filed in a nearby office bookcase. More typical are unscheduled backups using seat-of-the-pants methodology onto a variety of media including: memory sticks, CDs, and Zip drives with no verification, cataloging or periodic testing.

A dentist in Scottsdale, Arizona learned first-hand the dangers of not properly backing up records. After a hard drive crash, he checked his backups and found that his administrative assistant had, for two years, dutifully executed weekly backups...of folder shortcuts. After spending \$8,000 on forensic analysis, he was able to retrieve enough data to stay in business. Other common issues include misplaced or damaged tapes, discovered only after the original data was lost.

Strategies to protect your data

When it comes to data protection, small business owners typically are not interested in the latest revisions of a specific technology. Their concerns are more of a practical nature: stay in business, enjoy convenience and have peace of mind.

In order to achieve this, many small business owners see the value of outsourcing data protection to a professional. Many IT pros will take the time to understand the concerns of each particular business they service and are able to personally tailor solutions that meet its needs and budget. More importantly, IT professionals are able to fine-tune and check systems for proper functioning on a regular basis.

The ideal plan would include protection of computer systems from attack by viruses, physical protection of the hardware and stored data and backup to a remote location. Also important for small business owners is that the plan be as simple and automated as possible, freeing them to run the business, not become a technology guru.

Questions to ask before investing

"My first question was how much was it going to cost to get started and to protect my data on a monthly basis," notes Landa. "It's like insurance, you don't want to spend the money until you need the service. Then you are glad you have it."

Small business owners should ask these questions before investing in any data backup solution:

How much time will it take?

For small business owners, data backup should be automated as often as possible. Several solutions offer "set-it-and-forget-it" options that allow your backup to continue on a regular schedule with no human interference. Some offer a confirming e-mail to the business owner that assures them the data is backed up safely. This offers continued peace a mind.

Will a copy of the data be safe in the event of theft, fire or natural disaster?

Data that is stored on disks and drives is useless if those storage items are subject to the same disaster as the computer. The safest solutions include backup to a remote commercial data centers.

Will the data be encrypted to limit access on a stored tape or via Internet transmission?

Typical copying of files to CD or backup to tape can increase the risk of data compromise if the data is not encrypted. Any Internet data transmission is vulnerable if it is not encrypted.

What is the process for recovering the data?

Be sure to understand and test the system for ease of recovery before disaster strikes. Keep a copy of passwords and an outline of the recovery process in a secure location.

Who can you call for help in the event of data loss?

Find out if there a professional on call who understands your particular business.

How much will it cost?

Depending on the solution, an automated, encrypted remote data backup service may run from \$15.00 per month and up depending on the amount of data stored. Expect to pay \$2.50 per gigabyte or more.

Steps to protecting your data

There are several good practices any computer user can utilize to operate safely. Now is always a good time to minimize the risk of a data disaster.

1. Clean out old files. Throw out or store what you don't need anymore including old e-mails. Clutter can cause your system to slow down and even crash.
2. Update any anti-virus software, spyware and firewall protections on all of your computers. This will help protect you against one of the most common causes of computer failure.
3. Implement a data backup process that encrypts and stores your data in a secure remote location.
4. Update passwords and review the list of who has access to your data. People's roles change within your company and so will their need to access your data.
5. Make sure to keep the original software disks for your computer and other programs. This will make recovery easier in the event of data loss.

Data records can be the key to the success and livelihood of any small business. It is imperative they be properly cared for and protected from potential disaster. Don't wait until it's too late. Explore options for system backup that suit your small business needs today and prepare for tomorrow.

About the author

Jim Walker is President of DataPreserve Franchise, LLC, Scottsdale, AZ.

This article provided by:



1106 2nd Street
Encinitas, CA 92024
760-632-0068
info@peisersolutions.com
<http://www.peisersolutions.com>

Please contact us for all your data backup needs.