

Data Backup – How do you *really* fare?

Written January 2010 by Dave Gardner

As a technology consultant for over 30 years it amazes me how so many people have the false illusion that their data is safe and backed up. Of all the companies I have looked at over the years I would say that more than half have very poor, if any real protection. The biggest problem is that most don't fully understand the true risks and the recovery processes involved with data. Here are a few questions that everyone should ask their IT people. How many can you answer yes?

How reliable is you data where it resides?

- Is your main server secured in a locked controlled access room?
- Does the server require a login ID and password to gain access?
- Is the data stored on a RAID disk device so it keeps running even when a hard disk fails?
- Is your equipment protected with a UPS and does it perform automatic shutdown?
- Is the server kept clean and completely dust-free?
- Is the server room kept at a reasonable temperature to protect the computers?

Has access to sensitive data been secured?

- Do all the computers in the office require a login and password?
- Is your server completely isolated from the Internet?
- Do you have a secure firewall in place on your network?
- Do you control all outside (Internet) access to your network?
- Is data storage secured to prevent bulk downloading?

Are your backups being done correctly?

- Are you doing backups at least daily?
- Are backups written on media rotated in daily, weekly and monthly cycles?
- Is the backup stored off-site every day?
- Do you have a device to read the backups off-site on another computer?
- Are you fully testing the backups on a remote computer at least monthly?
- Is your off-site backup storage secure and is the backup data encrypted?

A few more questions worth asking:

- Do you backup all your data before you do any upgrades to computers or software?
- Do you have a specific permissions and access levels for each of your employees?
- Have you ever had an outside IT specialist audit your IT infrastructure?
- Are all keys, login ID's and Passwords kept secure (not on sticky notes in desk drawers)?
- Do you change office keys and passwords on a regular basis?
- Do you have an employee dismissal checklist and security plan?

If you can answer all of these yes then you are probably in good shape. If you don't fully understand them, ask someone. Get straight answers and second opinions. It's your data and your business. The loss of data can be catastrophic and can easily lead to the demise of a business. Even if you use outside professional organizations – ask the questions.

Dave Gardner is CTO for DeskTop Business Solutions (www.dtbusiness.com) developers of LAWS/Pro a Cloud-based application which performs time, billing, accounting and document storage for attorneys, accountants and consultants.