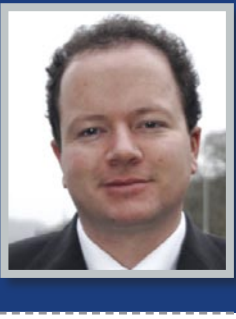
Backup! Backup! Backup!

The risks are really great



John Gleeson
Director, iThink Technology
Email: info@ithink.ie

One of the things that I cannot stress to customers often enough is that when it comes to preventive maintenance and system care, regular reliable data backup is of utmost importance. No matter how well you treat your system, no matter how much care you take, you cannot guarantee that your data will be safe if it exists in only one place. The risks are much greater than most people realize. How important is your data to you? You can respond to this question with words, but the steps you take to protect your data are the real answer. I find it troubling when people lose large quantities of data--because they have no backups--and then they get very upset, talking about "how important that data was!" If it's important, why wasn't it backed up? If it matters enough to get upset over losing, it's worth protecting, and backups are an essential part of data protection.

There are many reasons that people neglect backups:

- They don't understand how important they are, because they haven't had a disaster happen to them (yet).
- They don't know the technology involved.
- They forget to do them because they don't have a routine for doing backups.
- Doing the backup is an extra chore and so it is ignored.

Not only is it absolutely necessary to back up your data, but it is equally important to do it daily. Anything can happen at any time. Remember, you are dealing with a highly vulnerable medium that can be affected in numerous ways by any number of outside factors. As a result, your data can be lost due to something that is totally out of your control. There are software corruptions, viruses, lightning strikes that cause unexpected hardware damage, and so on. A user may accidentally delete your complete customer database or an irate employee may decide to delete all the accounts information. The thing about disasters is that you never know when, where or how they will happen. The more backup copies you have created, the better off you are when you find yourself in any trying circumstance which calls for the replacement of your data. If you have a recent copy of your data, it is a simple matter of restoring and you are back in business. If not, you may find yourself up the proverbial creek in a canoe without a paddle.

WHAT, WHEN, HOW:

The ideal business solution for storing data is that all data should be stored on a central server which is protected from disaster by additional hardware. (More on this next month.) No data should be stored on the workstations. Should data be required on laptops to enable employees to complete work offsite, the laptops should be configured to replicate the data back to the server when they are next connected to the office network. A complete backup of the server should be done onto tape each night by backup software that is configured to automatically backup to the tape. Each morning the tape should be changed for the following night's backup and the backup software logs should be checked to ensure the backup was successful. These backup tapes should then be stored off site (either at home or in another building) or in a fire proof safe to protect the tapes from fire damage in the worst case scenario.

For smaller businesses without a central server data maybe spread across several PCs or laptops. This is a harder scenario to deal with but none the less backups must be done. Ensure that all users store their data in the one location i.e. "My Documents" on their PCs/ Laptops. Ensure that all users have access to some form of backup media such as writeable CDs, DVDs, USB memory sticks or external hard drives. Inform all users of the importance of backing up and ensure they are all aware of the procedure to backup their data to the required media. Provide them with a backup sign off sheet to ensure that all backups are logged in case of a disaster so that you know when a file can be retrieved from. If possible automate the backup procedure as much as possible by using the inbuilt backup software on the PC or by purchasing backup software. The more automated it is, the more likely it will be done. Remember humans forget, ignore and defer. Computers do not.

What ever backup solution you implement make sure that it is tested on a regular basis. On many an occasion I have being requested to restore a system and being handed a tape that has been used for nightly "backups", only to find that the tape is blank or the data is 12 months old or that the contents is corrupt! Just because you replace the tape in the backup drive each morning does not mean the nightly backup has completed successfully. Backup logs must be checked to ensure that the backup completed with errors and test restore should be carried out on a regular basis to ensure that the tapes can be read from.

That's it for this month. In the next issue I will be covering the benefits of a central network server.

Should you require any further information or advice on any of the topics covered please do not hesitate to contact me at jgleeson@ithink.ie