Time to Think About Backup

An AbleIT Whitepaper

October 1, 2014

Prepared By:

AbleIT Inc.

**8148 – 46th Street
Edmonton, Alberta T6B 2M8
587.523.2252**

Time to Think About Backup

It's a term we hear quite often…Backup. But what it is it, what does it mean when we say Backup? There can be many different ideas of what backup is…but it comes down to one very basic principle. That principle is to safe guard your corporate data so that if anything happens; a disaster strikes, viruses, disgruntled employees, anything that has the potential to cause the interruption of your business; your business can recover and continue operations. Backups will allow you to recover information that your business needs to operate; email, file data, employee information, and so on the list goes. In case of an interruption, corruption or loss, backups help recover information.

This information makes your business what it is, allows it to operate and grow as a business. This includes word processing documents, spreadsheets, email, presentations, videos, images, scanned documents and many other forms of data. Organizations today generate large amounts of data, many of which are business records and other content that are critical to your business's operations. Imagine coming to work one day to discover that **all your data is gone**. How will you recover from this, all the while trying to maintain your current business obligations? Many businesses rate backup towards the top of the priority list, but still, a third of businesses do nothing to back up their data.

Remember this: It is quite easy to lose data…and all but impossible to rebuild that data if backups do not exist. Businesses are much more likely to recover from a disaster with solid backups in place.

Let's take a close look at Backups to get a bit more information.

Types of Backup

There are several types of Backups that exist. First, we will look at two different storage options for backups: local and offsite.

The first backup type to discuss is a **local** backup. This is a backup strategy that backs your data up to a device that is inside your business. This can be a backup server, or a backup hard drive or backup tape. It can be as complicated or as simple as you want. This type of backup is a good place to start, and will help you recover files that may have been deleted or altered, or data that has been lost, such as a laptop theft. However, this backup is only good if your facility is operational…if something happens to make your facility inaccessible, your backup is also inaccessible.

This brings us to the second backup type to discuss; **offsite** backup. This is a backup strategy that backups your data up to a device that is not stored at your business. This could be a cloud service, such as the type we offer through AbleIT, or it could be as simple as an external hard drive or tape that somebody removes and takes with them. Some businesses have an offsite storage facility, such as a warehouse, which they can take these devices to for storage. Ensuring the facility is **safe and secure** is very important. Business owners who have been impacted by natural disasters, such as Hurricane Katrina, learned a hard lesson about keeping remote backups of their data.

Many places use local and offsite backups in combination. This is good for ensuring a second copy of your data is kept safe and intact, so if a disaster wipes out your office, you can go to your offsite location and retrieve your backup devices for recovery.

Backup Rotation Schemes Types

Next, we will look at one of the more common backup rotation schemes that are used.

A backup rotation scheme defines the method you use to back up your data. A rotation scheme is utilized to minimize the number of media used, such as hard drives or tapes, and determines not only how the media is used, but also when each piece is used for a backup job, as well as the retention period for said backup jobs. There are several backup rotation schemes that are utilized, the most common being the Grandfather-Father-Son backup scheme.

Grandfather-Father-Son Scheme

This backup scheme refers to a common rotation scheme for backup media. In this scheme, there are three or more backup cycles, such as daily, weekly and monthly. The Daily backups are rotated on a daily basis and are referred to as the "Son". Weekly backups are completed on a weekly basis, and are referred to as the "Father". Monthly backups are completed on a monthly basis, and are referred to as the "Grandfather".

This backup scheme will regularly produce a series of backups, covering daily, weekly and monthly time periods. Potential benefits of this backup scheme are listed below:

- An archive of daily, weekly and monthly backups will be created
- All daily backups will be available for 7 days after they are completed
- Weekly backups are stored for a full month
- Monthly backups will not be deleted and will be available for a full year

This scheme could be taken a bit further by introducing quarterly, half-yearly and annual backups. This would allow for some of these backups to be completed offsite, or backed up to a device and removed offsite for disaster recovery purposes. Executing backups using this backup scheme will reduce the time to recovery in the event of a disaster, which will provide better business resumption time.

What Should be Included in Backup?

When making the determination of what to include in your backup strategy, think of what your business could not function without. This may include a database, or a series of databases, spreadsheets, etc; each business will be different and will require a different combination of data to ensure business continuity. Anything that your business could not operate without needs to be included in your backup strategy.

Ideally the best backup includes **everything**. Having complete images of your servers backed up will reduce the time to business resumption considerably.

Testing the Backup

A backup strategy is the first step to ensuring your business data is backed up. An integral part of a backup strategy is to test these backups. This should be tested at least once a month to ensure your data is being backed up properly. A full test should consist of a restoring a specific set of files, and then compare the restored data to the live data to ensure it is a match. Once you have confirmed that the two sets of data match, your backup integrity is confirmed.

Ensuring your backup integrity before a disaster strikes will ensure faster turnaround time in the event of a disaster. This will in turn provide better business resumption time after a disaster.

Ask your IT provider…when was the last time your backup data was tested for integrity?

Consequences of no Backup Strategy

Failing to backup data can have disastrous consequences for a business.

Let's have a look at some backup-related statistics for a moment:

- 80% of businesses that experience a major disaster go out of business in three years (*Source: www.usfst.com "Hidden Threats to Enterprise"*)
- 40% of businesses that experience a critical IT failure go out of business within one year. (*Source: www.usfst.com "Hidden Threats to Enterprise"*)
- Businesses that are not able to resume operations within ten days of a disaster are not likely to survive (*Source: Strategic Research Institute*)
- 20% of small to medium businesses will suffer a major disaster causing critical data loss every 5 years (*Source: Richmond House Group*)

Loss of data brings enormous consequences to your doorstep. The smallest impact that this loss will have on your business is that users must rekey in lost data – assuming they are able to do so. This may lead to project delays, missed deadlines, lost sales opportunities and unhappy clientele. Not to mention productivity loss, as well as disgruntled employees.

Losing data can potentially have more serious consequences. What if the data lost cannot be recovered? The inability to recover lost intellectual property, data generated by former employees, missing email or missing accounting records can create serious problems on many levels, and may have ramifications that exceed the productivity loss that can result from data loss.

The potential costs of not having a backup can be astronomical, and can increase exponentially. Not to mention your business reputation may be impacted, and you may lose productivity or clients due to this failure.

Is it time for your business to think about backup? Does your business have a backup strategy in place? When was the last time this backup strategy was tested?