

Backup Strategies for Small Business

StarTech Group, Inc.

Jim Scalise

11.15.2014

CONTENTS

BACKUP STRATEGIES	1
CLOUD BACKUP	2
REMOTE DISK BACKUP	3
PROS AND CONS	4
CONCLUSIONS	5

Backup Strategies

Overview

Backing up your company data is the first step in the big picture for a disaster recovery plan for your business. The backup process should provide for a way to fully recover your data if you were to experience a catastrophic failure of your server. The key to a successful backup strategy is *“How fast can I get my server back online so I can get back to work”*.

A catastrophe could be defined as: a fire in your building, smoke damage, lightning strike nearby, flood, hurricane, theft, server failure, tornado, hacker and even a terrorist dirty bomb. Now most of these catastrophes would rarely happen, the most common that we have been involved in are lightning strike, hacker, theft and server failure. Any one of these catastrophic events could put you out of business. If you fall under HIPAA, then you could also incur a hefty fine for not safe keeping your patient data.

We are going to explore in this white paper the two most popular backup methods currently being used by small to medium size businesses. We define a small business as dental office, doctor’s office, insurance company, manufacturing company, retail or any company with less than 50 users. A medium size business would be a company that has between 50 and 300 users.

Cloud Backup

Cloud backups have been around for several years and have become quite popular due to their overall cost and ease of setup. There are now two versions of cloud backup solutions that have emerged – personal cloud backup and business cloud backup. The differences are outlined below.

Personal cloud backup is limited to static files and documents. Some examples of static files are pictures, music, Word documents, text files, spreadsheets etc.

Business cloud backup includes all of the personal cloud backup but can also backup Microsoft Exchange email database and Microsoft SQL databases plus databases from other vendors.



When deciding on the cloud backup solution most people will opt for the lowest cost which will always be the personal version which will not backup your business databases listed above.

In both types of cloud backup solutions you have the ability to encrypt the data that is stored in the cloud. Most companies will also provide for snapshots of older versions of your data so that you can recover a file that may have been changed or deleted accidentally.

If you are a medical/dental/chiropractic office, your needs are dictated by HIPAA. HIPAA requires the safe keeping of patient data. This means that the patient data has to be encrypted and safe guarded from theft or unauthorized access.

Removable Disk Backup

Removable disk backup is referring to a USB hard drive and locally install backup software. This type of backup allows for a full server backup which will capture all your data all software and the Windows operating system.

This type of backup will allow a full server backup to automatically take place every night when the office is closed. It is best designed in a Monday through Friday five day rotation to allow a restore going back five days.

Backup hard drives using a USB connection are fast, inexpensive and portable allowing you to take the backups off-site for safe keeping. And again, if you are a medical/dental/chiropractic office, your needs are dictated by HIPAA. HIPAA requires that the data is encrypted and kept safe from unauthorized access.

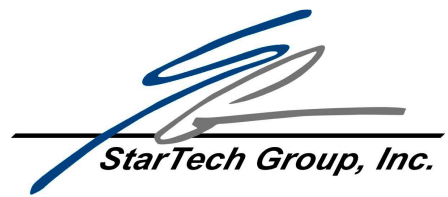


The proper procedure for safe keeping would be to also remove from the building all backup drives that are not currently being used. These drives should be kept off-site in a locked area or safe to protect them from fire or theft.

To provide for the backup to be encrypted you should purchase a server based backup software that has this feature. The backup software that comes with all Windows servers does not provide for encrypted backups.

The server where your software and data reside should use server grade backup software with these minimum requirements:

- a. Ability to backup all files and databases used by your business
- b. Backup the Windows operating system
- c. Ability to provide an email report on the status of the backups
- d. Ability to encrypt the backup to protect your data in-case of theft



- e. Ability to do a “Cold metal restore”. This is a process to take a CD created by the backup software and the last known good backup and restore the entire backup to new server hardware.

Pros and Cons

There are many pros and cons when it comes to backing up your server. Each business needs to determine what the best solution is for them. Below I've summarized the pros and cons for each type of backup solution.

Cloud Backup

Pros: Cloud based backup is a monthly service which is setup to automatically backup the data you have selected. It is a set it and forget type of technology. The cost is based on the amount of data to be backed up per month.

Cons: Unless you subscribe to the business version (more costly) you will most likely not be backing up your business databases. The cost to backup will increase over time as your data needs grow. Cloud based services are becoming increasingly insecure as hackers have found ways to penetrate these secure sites.

One important aspect of cloud backup that most people tend to forget is *"How long will it take to retrieve all my data when I have a failure"*. Unless you have an agreement to have your cloud vendor send you a USB drive with your data (an additional cost), you will be forced to download all that data. Depending on the amount of data and your Internet speed this could take days to complete.

Removable Disk Backup

Pros: Fast backup and restore of the entire server. All data including Windows operating system, installed software and all data including databases are backed up. No additional costs once software and backup drives are installed. Restore takes as long as the backup takes; hours instead of days. Ability to restore entire server to new hardware in hours – this is not available with cloud backups.

Cons: Initial cost for backup software and hardware. Over four years this cost would actually be cheaper than a cloud backup.

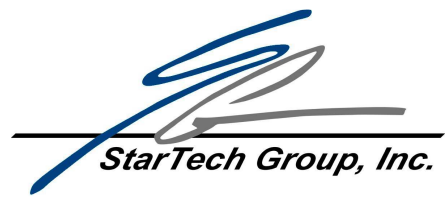
Final Thoughts and Recommendations

Over the 13 years we have been in business, we have tested and evaluated many backup solutions from several vendors. Our philosophy when determining the best backup solution is to look at the big picture for our clients.

We look at the backup as a part of a disaster recovery plan. We interview our clients to determine what would be an acceptable “*down time*” in hours for their business. How long could you work if you could not access your business data?

Most business would feel some pain after one hour and most would be severely impacted by eight hours of downtime. These same clients would be out of business if they could not access their data for four or more days. Employees would not get paid for this downtime. Their clients would look elsewhere for their needs. Lawsuits might be brought in some cases.

After evaluating cloud verses local disk backup, we determined that in all cases the cloud was deemed not a primary tool for several reasons which are listed in the cons. The cloud could be used for a secondary means of backing up business that like redundancy. Local disk backup cost about the same over a four year period, is much faster on backups and restores, provides for a full server backup saving time and money and is more secure as you have control over where your data is kept for safe keeping.



THANK YOU.

FOR MORE INFORMATION CONTACT:
JIM SCALISE
jim@startekgrp.com