3Fold IT

What You Should Know About Cloud-Based Data Backup

An Executive's Guide to
Data Backup and Disaster Recovery

Matt Zeman
3Fold IT, LLC
PO Box #1350
Grafton, WI 53024

Telephone: (844) 3Fold IT
Email: **Matt@3FoldIT.com**
Website: **www.3FoldIT.com**

Executive Summary

Choosing to move a company's backup data to the cloud is a course of action that offers many potential benefits. The most important of these advantages involve cost, reliability, and security. This white paper provides an overview of what cloud-based data backup solutions entail, as well as some crucial points to keep in mind when looking for a service provider.

The key topics covered in this report include the following:

- How creating a cloud-based data backup system can save both time and money
- How the various types of cloud-based data backup services differ from one another
- What points should be considered when choosing a cloud-based backup service and how to make the decision as simple and stress-free as possible

Introduction

According to a 2014 report from Symantec, 30 percent of all targeted cyber attacks are aimed at small businesses.[1] That is a shocking statistic in and of itself. However, it is even more surprising when compared to another figure from the National Cyber Security Alliance, stating that 60 percent of small businesses are forced to close within six months of an attack on their computer systems.[2]

These statistics show how critical it is for companies to establish a data backup protocol. The reality for many businesses is that they can lose their data without any warning. This can include any or all of their client lists, bookkeeping information, contacts, projects, and documents.

One example of such a situation involved businesses operating in Manhattan's Financial District right before Hurricane Sandy. Overnight, their offices were flooded, their computer equipment was destroyed, and any data on the premises was completely gone. While this was not the work of a hacker, it was no less devastating.

> Six out of every ten small companies hit by cyber criminals are forced to shut down within six months of the digital attack.

Data security is vital for small business owners, even when the survival of their enterprise is not at stake. Archiving data is essential to industries with complicated compliance rules or regulations, and can be especially helpful during litigation. Simply allowing old data to disappear over time can be the difference between winning and losing a lawsuit.

There are hundreds of ways to lose all of a company's data instantly. At best, it can cause an inconvenience. At worst, it can be crippling. The undeniable fact of the matter is that a data backup solution is essential for creating any strong risk prevention and disaster recovery plan.

The Basics of Data Storage

Of course, there are many different options available for backing up a company's data. Picking the right method is nearly as important as choosing to create a backup plan in the

---

[1] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[2] http://www.staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic

first place. There are three main approaches to digital information management: in-house, traditional off-site, and cloud-based.

In-House

In-house data storage solutions are generally the most complicated option, but they also provide the most control over every step of the archiving and backup process. In-house solutions are best for large, established businesses with complex data needs and a specialized IT department.

A good in-house plan also has back-up systems in place at off-site locations. These contingencies are established so that an organization can recover in the event of a serious disaster such as a fire, flood, or earthquake. For the sake of efficient redundancy, backups usually consist of both digital and physical copies of data.

Traditional Off-Site

The traditional off-site storage plan is what most people think of as "data warehouses." Data is usually stored in a digital form locally, and then transferred to physical formats such as tapes before being taken off-site.

For the last several decades, off-site solutions have been the mainstay of businesses looking to back up their data. However, traditional off-site solutions suffer from some serious drawbacks, including the time and effort required to transport the backed-up files and their vulnerability to physical damage in the case of a natural disaster.

Since cloud-based data backup plans are entirely digital and require only an Internet connection, they are far more flexible than other methods.

Cloud-based

Cloud-based solutions offer businesses a convenient and safe way to store their information. This approach involves transferring data to multiple remote servers. Information is stored digitally the entire time, and because it is distributed across servers in multiple data centers, it is much less likely to suffer from any kind of loss.

Backup Methods and Frequency

Backup procedures can be implemented in multiple ways, each with their own advantages and disadvantages. There is no "right" procedure, because a company's backup schedule and type should be chosen based on its individual needs.

Since cloud-based data backup plans are entirely digital and require only an Internet connection, they are far more flexible than other methods. This versatility makes the issue

of frequency much simpler, because businesses no longer have to plan physical media deliveries or pickups.

Establishing the appropriate schedule for backing up data largely depends on the methodology. The main types of backup processes are full, differential, incremental, and continuous sync.

Full Backups

The full backup is what most people typically imagine when they think about backing up their data. It involves regularly copying the entire contents of a designated data source – whether that is a desktop computer, laptop, or server – and moving all of the files collectively as one single backup unit.

> Combining a cloud-based approach with the performance of full backups on a regular basis offers companies a comprehensive level of security and reliability.

This process is often slow. Due to the fact that everything is copied, it is usually performed after business hours, when the machine being backed up is no longer in use. Often, a copy, or "image" as it is known in the IT industry, is made of the entire hard drive. This ensures that if anything should go wrong with the machine, the image can replicate the original perfectly.

While the full backup plan is an excellent way to protect a company's data, it is not good at dealing with files that often change throughout the day. The large amount of time needed to perform a full backup means that it is usually only run once during any given backup period.

This means that any changes made between copies could be lost if something were to happen to the source machine. A full backup is also very intensive from a memory and bandwidth perspective. The protection offered by a full backup often comes with the added cost of having to pay for significantly more storage space. Since the information has to be transferred to the backup facility over the Internet, an extremely fast connection speed is required.

For these reasons, full backups are rarely used as primary day-to-day data-preservation mechanisms. Instead, they are reserved for longer time periods, such as weekly or monthly updates. Even if a cloud-based solution is in place, businesses should consider doing a full backup every month or two.

Differential Backups

Instead of backing up all of a company's files every time, the differential method only copies files that have changed since the last backup. This system has several advantages over the full backup.

The main benefit of a differential approach is that it requires much less storage space, bandwidth, and time. Instead of copying the entire hard drive regularly, only certain, commonly used files are backed up every period. This makes for smaller "pieces" that need to be copied and transferred to the storage center.

The disadvantages of the differential backup method present themselves at the data-recovery phase. Depending on the system in use, it can take data from multiple backup cycles in order to fully recover all of a company's records.

> A sound disaster recovery plan should feature daily – or even more frequent – backups.

Since each backup only comprises the changed files, differential backup systems often require specialized software in order to reconstruct all of the various pieces into an accurate image of the original hard drive. It can also take significantly longer to download all of the pieces needed for a complete recovery.

Incremental Backups

Incremental backups combine the best, and some of the worst, of both worlds. In an incremental system, full backups are scheduled over longer time periods, typically either weekly or monthly. At the same time, differential backups are run daily.

This system allows an organization to recover files more easily, since it will only need to recover the last full backup and all the incremental ones since the full backup was taken. This process is faster and more reliable than the differential backup, and requires less time and storage space than the full backup.

Continuous Sync

Unique to cloud-based data backup storage services, continuous sync backups make the entire process simple and constant, with very little chance of losing data. The information is backed up in real time to the cloud as files are modified, and any lost files are also recovered in real-time. This is the backup system commonly used by personal cloud storage solutions.

Because files are backed up constantly, there are never more than a few minutes of time that can be lost in the event of a system failure. Additionally, recovery is simple, automatic, and usually invisible to the end user.

The major drawback to the continuous sync system is that a constant web connection is needed for the backup to take place. However, most systems are intelligent enough to track changes when no network is present and then upload all of them to the cloud when the machine becomes connected.

How Often Should A Backup Be Performed?

A sound disaster recovery plan should feature daily – or even more frequent – backups in order to ensure that data is not lost in a worst-case scenario. Cloud-based backup solutions have greatly simplified this process by offering a continuous backup system that stores files as they are modified and created. Nevertheless, regularly scheduled full backups are still recommended for redundancy and ease of recovery.

No matter what type of system is in place, letting more than a month, or in some cases days, pass between backups places a company's data at serious risk of being lost.

Data Recovery

The essential premise of a data backup system is that it ensures the safety and availability of data if a recovery is needed. To that end, an effective backup solution is one that allows for a quick and easy recovery.

Data backup systems provide several recovery options. The best solution for users is always dependent on the situation, with different recovery methods only available for specific types of backup systems.

Manual Recovery

Traditionally, backups were performed manually at predetermined intervals. There was no way to back up large amounts of data, since backup copies were written to a physical medium.

These copies needed to be frequently replaced and then transferred to a secure storage facility for archiving. In contrast to this, the cloud-based data backup method moves the process to the Internet, thereby removing the physical media entirely.

Modern-day manual recoveries can be performed at the request of the user, and often offer choices as to how far back a recovery should go. This option offers flexibility and can often be used to perform incremental recoveries, where only certain files are restored. Manual recoveries are particularly helpful if a virus infected the source machine, since users can recover data from a time that predates the attack.

Cloud-based backup service providers that perform full hard drive imaging will sometimes offer image virtualization. This lets users open a backup image on the provider's servers as if it was a perfect copy of the original hard drive. This can save a lot of time and bandwidth, since users do not have to download the whole recovery image.

Automated Recovery

An automated recovery system allows the user to set regular intervals for automatically backing up a hard drive. It will scan the user's machine for data loss, and then recover the

files that were damaged. When it cannot restore the corrupted files, it will prompt the user to perform a full recovery.

This is very similar to how the Windows Recovery system works on local machines. In essence, it makes the process of recovering files either a completely seamless action or a simple maneuver that only requires a few clicks.

One downside to automation is the fact that users lose some level of control regarding what gets recovered and when. However, this approach does not require any long-term input from the user. As a result, it makes the process much easier for employees, especially those working remotely or on laptops.

Human Error

Instead of bringing their machines to an IT department or having to remember to run backup software, users of an automated system can set the schedule once and then forgot about it. As a result, an automated solution largely eliminates the possibility of human error, so long as the machine remains on during the scheduled backup time.

However, even automated systems are not without some dangers. The most noteworthy of these involves failing to properly configure the system. While human error on manually backed-up machines may cause one or two copies to be lost, a poorly configured automated solution can fail to back up any data at all. Even worse, an improperly implemented automated system will fail silently, meaning that the failure will not be noticed immediately. This could potentially cause months of lost data.

Even with automated cloud-based systems, regularly performing full manual backups is highly recommended.

An automated backup attempt will also not work if the system loses its network connection or is turned off during the scheduled backup time. Thankfully, monitoring software can usually catch these mistakes before they cause any problems.

Even with automated cloud-based systems, regularly performing full manual backups is highly recommended. It is a good rule of thumb to establish full, manual backups every month or two. System administrators should also verify their cloud-based backup solutions on a monthly basis. This hybrid approach works to eliminate the shortcomings of both manual and automated systems.

Comparing Cloud-based and Traditional Services

Cloud-based backup solutions offer many pros and cons, but to judge them fairly, they need to be compared to traditional backup options.

Cost

One area where cloud-based data backup solutions really shine is cost. Generally speaking, they are significantly less expensive than traditional backup and archiving methods. They also have the advantage of being very scalable, with many providers offering "pay-for-use" plans that let a customer pay per gigabyte of backed-up data. This lets users alter their approaches, as their backup needs change.

> Business owners should ask about a service provider's uptime guarantee and plans for system maintenance.

Traditional off-site backup plans, on the other hand, involve buying server storage space in preset amounts. As a result, businesses often have to buy packages that greatly exceed their needs, and therefore pay for space even if it is not being used.

Cloud-based solutions also trump on-site backup systems in this regard, since the latter requires a large capital expenditure on servers, software, and physical media. Cloud-based services also cut IT personnel costs, as they rarely require a data storage specialist.

Reliability

Cloud-based storage systems have distinct benefits and detriments when it comes to reliability. On the positive side, all reputable cloud-based backup providers offer a service level agreement (SLA) that details how reliable the system is guaranteed to be.

The key sections of an SLA are the uptime guarantee, and the amount of planned maintenance. The latter is explained below. The former, on the other hand, refers to the amount of time that the provider guarantees that the network will be available. Business owners should be sure to ask about these points. If the service provider cannot or will not provide the information, then business owners should consider choosing a different company.

Planned maintenance refers to the system downtime that is designated for upgrades, repairs, and general refreshes. A consistent maintenance schedule keeps the system running smoothly and without hitches. Any downtime as a result of planned maintenance should be barely noticeable. Generally, these efforts are scheduled for periods of relative inactivity across the system, such as very early in the morning.

Unplanned downtime happens if something in the system breaks or needs emergency repair. Most cloud-based systems are built with enough redundancy to ensure that these kinds of events remain unnoticed by the consumer. Still, it is important to know that since a user does not physically control the data, there might be brief periods of time when it is inaccessible.

When it comes to reliability, traditional off-site backup solutions bear a few similarities to their cloud-based counterparts. Both generally have some planned downtime, and both can suffer from unexpected difficulties. The main difference is that cloud-based systems generally have much more redundancy, with the data being mirrored across servers in multiple locations. This translates to a much lower risk of a total outage.

In-house solutions are far more prone to problems, since the data is located in one place. Often, this location is close enough to the main offices such that any catastrophic event, such as a major hurricane, will knock them out of commission as well. However, this proximity is also an advantage, because it makes a full recovery much quicker than downloading the recovered files from a remote server.

Safety and Security

Cloud-based data backup solutions are generally safer and more secure than traditional backup measures. Service providers provide this level of security through several means.

Because of the way cloud-based storage works, multiple copies of a company's files are kept on servers in several different locations. This redundancy keeps the files much safer in the event of a major disaster or server failure. In most cases, they are also heavily encrypted. This keeps the contents of the files safe from spying and alteration. The encryption runs from end to end, meaning from the minute the backup is created to the minute that it is recovered.

The main disadvantage with cloud-based backup systems is that a user does not have complete control over the data.

Many cloud-based service providers cater to companies governed by extensive regulations. These businesses typically include law offices, banks and financial institutions, and medical practices. Customers should make sure to instruct their service providers about any industry-specific rules that need to be followed.

The main disadvantage with cloud-based backup systems is that a user does not have complete control over the data but is still liable for any security breach. For example, a medical office – and not the service provider, as long as it complies with the applicable standards – would be liable for breaking the law if a patient's information was accidently published online.

These liability concerns are present in all backup solutions. On-site backup systems are still vulnerable to intrusions, losses, and thefts, as are off-site physical storage options. However, compared to cloud-based approaches, they offer a user more control over the data.

Conclusion

For most businesses, a cloud-based data backup service is the ideal balance of risks and rewards. It provides as much, if not more, reliability as both in-house and traditional off-site backup solutions. In addition to this advantage, cloud-based options offer a high level of scalability and security at minimal costs.

A strong disaster-recovery plan is essential to mitigating risks. Using a cloud-based data backup solution as the cornerstone of that plan is a good way to ensure that small-business owners are not caught off-guard the next time disaster strikes.

About 3Fold IT, LLC

3Fold IT was founded in 2006. Since our formation, we have helped hundreds of customers throughout Wisconsin improve their mobility, be more productive, and protect their data and IT hardware.