A PRACTICAL GUIDE TO CLOUD BACKUP

STAGE2DATA

CONTENTS

1. INTRODUCTION

Organisations of all sizes struggle with storing, protecting and managing large amounts of data. Traditional storage platforms such as hard disks, flash drives and other types of physical storage devices have long lost their appeal and people are increasingly looking for more advanced options of cloud storage for their files and data. Technology is further changing the shape of business, which means businesses are seeking more ways in which to protect critical business data efficiently and effectively.

According to Forbes:

- **hybrid cloud adoption grew three times in the last year, increasing from 19% to 57% of organisations surveyed.**
- **In 15 months [July 2018], 80% of all IT budgets will be committed to cloud solutions.**
- **73% of companies are planning to move to a fully software-defined data centre within 2 years.**
- **49% of businesses are delaying cloud deployment due to a cybersecurity skills gap.**

Despite these encouraging statistics, storing, protecting and managing large amounts of data remain a challenge for most businesses. Businesses are generally not enthused when confronted with the reality of having to make changes to their business, let alone moving all their data to the cloud.

Organisations further grapple with common struggles in their quest to maintain the appropriate levels of physical storage that adds to the expenses associated with such storage capacity. The capital required for additional infrastructure exponentially adds up. Operational costs are a further factor to consider. Companies have to monitor backups to ensure these are executed timeously and successfully; they have to plan for failures, performance bottlenecks, and capacity upgrades. All of these require interventions from IT professionals that in turn divert their attention from engaging with strategic IT projects. A further issue for businesses that rely on traditional storage methods is how to manage removable media effectively. The longevity of the removable media and the security risks involved require regular monitoring along with effectively tracking tape budgets. Meeting increasing data storage requirements should also be considered.

Today's businesses generate vast amounts of data and struggle to keep up with growing storage requirements. This, in turn, puts increasing pressure on storage budgets and constrained backup windows. As reliance on IT increases, recovery times are reduced. A survey conducted by EMC Global Data Protection Index shows that the majority of organisations are not fully confident in their ability to recover after a data disruption. It follows, therefore, that ineffective disaster recovery management will leave organisations unprepared and unable to ensure business continuity in the event of a disaster. It is crucial for businesses to be able to seamlessly collaborate and share company information with employees and to address the challenges associated with increased data volume storage.

In this regard, the development of cloud storage eliminated the traditional risks associated with data storage, which led to an increased need for data storage space on cloud servers. Cloud servers deliver remote data storage services to subscribers who will be able to process all their data and files stored on these cloud servers and backup or recover the files they need on demand. The ability to access data from remote locations with only a stable internet connection, gives cloud storage an undisputed edge over other standard storage options. In addition, it is possible to have almost any technology running in the cloud.

This guide was compiled with the aim of first, educating business owners about cloud backup and secondly, providing a balanced overview of cloud backup, the different types of cloud backups, and the advantages and potential challenges. It delves into the history of traditional backups whereafter it compares it to current day technology, that is, cloud backup. Thereafter it expands on the types of cloud backups and highlights the advantages thereof. The final part draws a brief comparison between Cloud Backup and Business Continuity/Disaster Recovery and elaborating on the points to take into account when choosing a cloud service provider.

1. BACKGROUND OF CLOUD BACKUP

2.1 The history of backing up

"Although the century-old technology has disappeared from most people's daily view, magnetic tape lives on as the preferred medium for safely archiving critical cloud data in case, say, a software bug deletes thousands of Gmail messages, or a natural disaster wipes out some hard drives. The world's electronic financial, health, and scientific records, collected on state-of-the-art cloud servers belonging to Amazon.com, Microsoft, Google, and others, are also typically recorded on tape around the same time they are created. Usually the companies keep one copy of each tape on-site, in a massive vault, and send a second copy to somebody like Iron Mountain. Unfortunately for the big tech companies, the number of tape manufacturers has shrunk over the past three years from six to just two – Sony and Fujifilm ...".

What does "backing up to the cloud" really mean? One way to understand the history of backing up is to understand the evolution of the technology that preceded cloud backup. In what follows, the history of how the current online backups came to be will be outlined briefly.

2.2 The forms of backing up

Magnetic tape

German engineer, Fritz Pfleumer, first patented magnetic tape in 1928. It was based on the invention of Vlademar Poulsens' magnetic wire. However, it only entered widespread use as a medium for mass storage of computer data in the 1950s where it formed part of the so-called 'computer revolution'. One of the first practical high-speed tape systems was the IMB 726 of 1952. It used a vacuum channel system allowing the tape to stop and start almost instantly and could store 2million digits – a vast amount considering the time. The IBM 726 was sold together with IBM's first digital computer, the Model 701, which could be rented for $850. The drawback of magnetic tape was, however, that it could deteriorate through what is known as sticky-shed syndrome. It is caused by hydrolysis of the binder in the tape that ultimately renders the tape unusable. The hard-disk form of backup followed magnetic tape.

Hard disc

IBM introduced the first hard drive disk storage unit, the IBM 350, in 1956 and, by the early 1960s, the hard drive disk (HDD) became the preferred backup technology and is still in use today. Hard disks store data on rotating rigid disks (known as platters) coated with magnetic material, and use magnetic heads arranged on a moving actuator arm to read and write data to the surfaces. The 350 could store 5 million 6-bit characters (3.75 MB) and had fifty 24-inch (610 mm) diameter disks with 100 recording surfaces. Each surface contained 100 tracks and the disks spin at 1200 rpm. The data transfer rate is 8,800 characters per second. Several improved models were added in the 1950s. The IBM RAMAC 305 system with 350-disk storage leased for $3,200 per month. The 350 was officially withdrawn in 1969. Various other IBM HDDs followed before the introduction of the floppy disk.

Floppy disc

As computers became more prevalent and available to a broader audience (yet still too expensive for home use), the need for portable storage arose. This need was met when David Noble and his team invented the 1MB 8" floppy diskette. It was originally designed for the IBM 3330 (or, Merlin) but since the disc was lightweight and cheap and could easily be transferred, it gained mass popularity fairly quickly and became the default medium for computer storage. It remained popular well into the early 2000s where after it became less of a mass storage device and more of a means to transfer personal files.

Optical storage

James T. Russel first developed the idea of using light to record and replay music in 1965, but it was not until the late 1970s and early 1980s that Sony and Philips commenced serious work on the concept. In 1984, the first CD-ROM (Compact Disk Read-Only Memory) was produced that was capable of storing computer data on tiny pits etched into the plastic of the disk.

It was not until 1990, however, that the CD-Recordable (CD-R), also developed by Sony and Philips, was introduced, and the heyday of optical backup could begin. Cheap, easily transferable, readily disposable, and holding over 600 times as much data as a floppy disk (650MB), CD-R rapidly became the back-up solution of choice for home users. Over the last few years falling hard disk prices (including the introduction of easily portable external hard drives). Moreover, the introduction of solid state media (most notably increasingly cheap and capacious USB 'thumb drives'), has started to see optical storage falling out of favour as the home backup system of choice. Most importantly, the rise of cloud computing has revolutionized the field of backup storage.

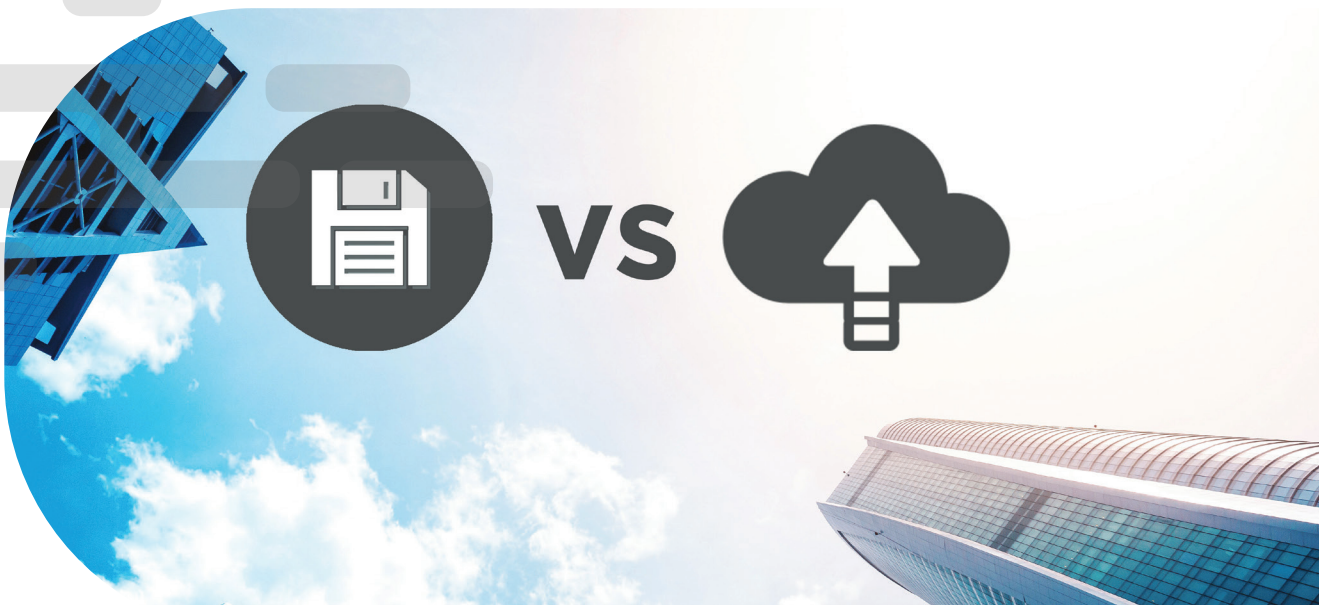
Online backup

Cloud storage is a model of computer data storage in which digital data is stored in logical pools where the physical storage extends across multiple servers and sometimes in multiple locations. The physical environment is typically owned and managed by a hosting company. These hosting companies (or cloud storage providers) are responsible to ensure the availability and accessibility of the data and furthermore that the physical environment is protected and running. People and organisations either buy or lease storage capacity from the providers to store user, organisation, or application data. In simpler terms: when a file is uploaded to the cloud, it is usually encrypted and transferred over the internet to another computer that is called a server that is attached to banks of HDDs. The data is stored on these HDDs that are typically arranged in RAID arrays in order to improve performance and mirror data across multiple drives. This method safeguards against data loss.

In light of the history above it is clear that the technology underpinning online backups are not entirely new. The combination of faster and more available internet plus cost-effective mass storage enables this concept. Instead of backing up data manually and storing it locally, the process in its entirety can now be automated with cloud backup and vast amounts of data can be stored offsite.

So how does the two forms of backup compare?

CLOUD BACKUP	TAPE BACKUP
simple, easy to download software, transfers are fast and runs as a background task	additional hardware is required, transfer of information is accomplished manually
restoration is simple and easy and the data is accessible from anywhere, at any time	copies of data must be stored in a different location to the server in the event of a catastrophic event that could damage the equipment or the building in which it is housed, require additional physical store space and manual restoration
reliable with a 99% restoration rate; redundancies in place to ensure the integrity of stored data	traditional tape backups lack the same level of certainty; over three-quarters of all businesses that use cassettes are unable to restore their systems successfully. The data corrupts overtime, making it unusable.
cost-effective	compared to cloud backup costs, tape backup costs are astronomical



3. TYPES OF CLOUD BACKUPS

3.1 Definitions

Private cloud

Private cloud – Private cloud services (also known as an internal or enterprise cloud) are used by a single organisation and are not exposed to the public. The cloud itself is situated inside the organisation and is protected by a firewall to ensure only the organisation and its users have access to the data.

Public cloud

Third-party providers offer public cloud services over the public Internet, making them available to anyone to use or purchase. They may either be free or sold on-demand, allowing customers to pay only per usage for the CPU cycles, storage, or bandwidth they consume. An example of a public cloud is Amazon Web Services.

Hybrid cloud

Hybrid cloud services use a mix of on-premises, private cloud and third party, public cloud services with interplay between the two platforms. It is often referred to as the best of both worlds.

3.2 Differentiation matrix

ATTRIBUTE	PRIVATE	PUBLIC	HYBRID
Tenancy	Single tenancy – only one organisation's data is stored into the cloud	Multi tenancy – more than one organisation's data is stored in a shared environment	A combination of both single- and multi tenancy where the data in the public cloud is still stored in a shared environment and where the organisation keeps the information stored in the private cloud private.
Security	Only the organisation itself can see and use the data in the private cloud services. This gives security-conscious customers peace of mind.	As anyone can use the public cloud's services, and as physical resources are shared, some organisations are selective about which workloads would operation on this cloud.	Only the organisation's users can access the services running on a private cloud, whereas anyone can access the services running on the public cloud.
Location of data	Inside the organisation's network.	Anywhere on the Internet where the cloud service provider's services are located.	Private cloud services – inside the organisation's network. Public cloud services – anywhere on the Internet.
Capacity	Computing, storage and networking resources dedicated to a single organization; limited supply matched to demand	Shared computing, storage and networking resources; limited supply but scalable to demand	A combination of both.
Cloud service management	The organisation's own administrators manage and maintain the services.	The cloud service provider manages and maintains the services since the organisation is only using the service.	The organisation itself must manage the private cloud, while the cloud service provider manages the public cloud.
Hardware	The organisation itself must provide the hardware and has to purchase the physical servers on which to build the private cloud.	The cloud service provider provides the hardware and ensures it is always operational.	For the private cloud, the organisation provides the hardware and for the public cloud, the cloud service provider.
Costs	Can be quite expensive, given the fact that the organisation itself is responsible for the hardware, applications, and management of the network.	The CSP has to provide the hardware, set-up the application and provide the network accessibility according to the SLA	The private cloud services must be provided by the organisation, including the hardware, applications and network, while the CSP manages the public cloud services.

3.3 Deciding on the best cloud option for your organisation

Organisations typically use public cloud services for:

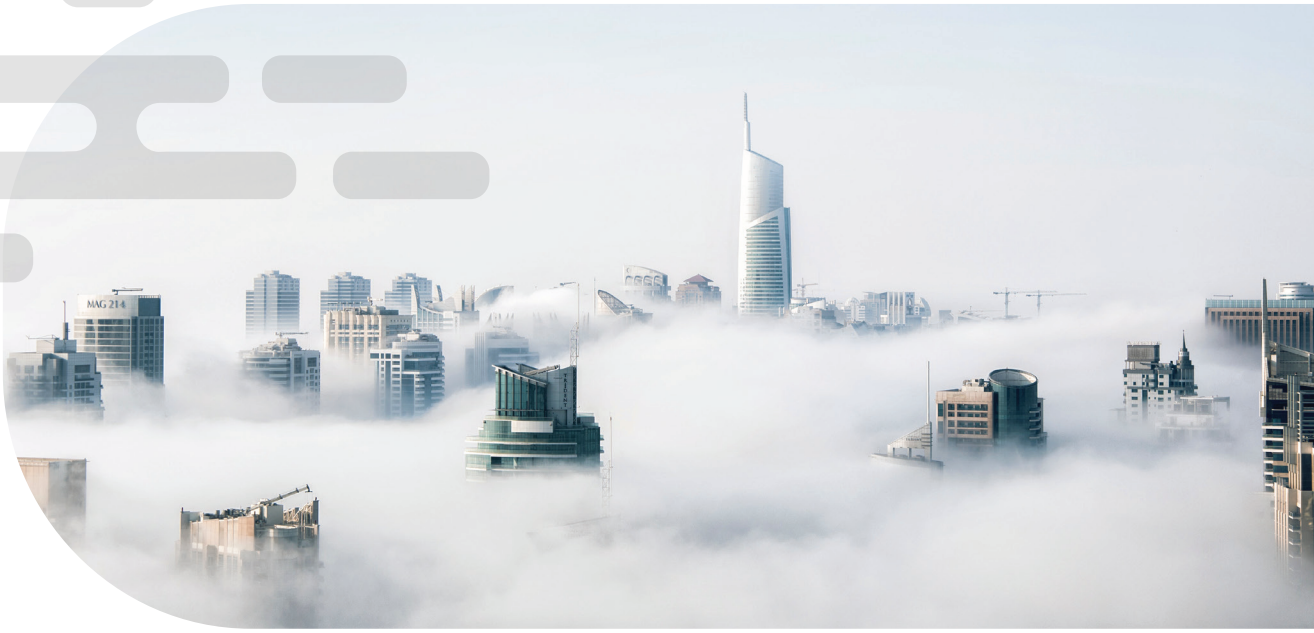
- **Quick deployment** – productivity applications and websites with high bandwidth pipes, high availability and auto-scaling capabilities to scale easily.
- **Extending IT** – high bandwidth connectivity combined with high performance computing services as an extension of the organisation's data centres.
- **Cloud bursting** – temporary increase of resources to accommodate short-term projects.
- **Disaster recovery** – cloud-based disaster recovery measures to ensure business continuity and short recovery time objectives (time to restore) in case of outage.

Some of the reasons why organisations use private cloud services include:

- **Compliance and security** – Organisations with requirements for compliance and data sovereignty or are hosting highly sensitive data.
- **Performance and control** – Organisations with applications that require high performance with low latency and those wanting direct control and oversight of their IT assets.
- **Business size** – Businesses with small IT departments or branch offices/ departments/ remote offices looking to set up new on-premises Cloud implementation or to share and standardise resources.

Hybrid cloud environments can keep data safe, secure and separate and allow data to move freely between private and public clouds. The hybrid cloud environment creates a flexible way to ensure increased options for data deployment.

4. FIVE ADVANTAGES OF MOVING TO CLOUD BACKUP



Businesses are increasingly moving to cloud backup, which makes a cloud backup platform that will ensure the safety and protection of your data non-negotiable. Failing to do so can result in your organization losing critical data through natural disasters or malware.

Below we have listed some of the advantages and benefits of using cloud backup:

- **It provides an additional layer of off-site data protection in the event of a disaster**

Every organisation should have a backup plan to cater for emergencies and to avoid losing crucial business data. Cloud backup creates a backup of all the files stored by the organisation. The data is then stored in a remote location where you can retrieve it at any time through an internet connection.

- **It is safe and secure**

Once the data is stored in the cloud, it is distributed across redundant servers safeguarding the data against hardware failures. Leading cloud backup service providers like Stage2Data use military grade encryption installed to ensure no one gets in. Cloud servers furthermore provide automated backups and snapshots to ensure further date safety.

- **It is automated**

Storing and processing applications and data in the cloud allow you to schedule data backups so as to not hamper daily business operations, which is a challenge for most business owners. Cloud backup simplifies the tedious task of backing up data manually on a daily basis. You select what you want to backup and when you want to run your backup, and the cloud takes care of the rest.

- **It is cost effective**

You can reduce your annual operating costs as well as your bandwidth costs by switching to cloud storage. Further costs savings can be achieved, as you will not require internal power and resources to store or maintain data remotely. The cloud is affordable and proven to be the most secure way to backup critical and archived data.

- **It is easy, accessible, up to date and reliable**

Cloud backup does not require an additional time commitment from you or your customer. Computer files are backed up to the cloud automatically and continuously, whenever you're connected to the Internet. Having data in the cloud ensures your customers have access to their data at any time and from anywhere provided they have access to the Internet. Users can easily drag and drop files into the cloud and no technical knowledge is required from users to be able to use the cloud effectively. Cloud backup solutions have made continuous management and restoration easy; with just a few clicks, backed-up data can be located and restored from anywhere in the world.

Cloud storage can also help your company reduce its carbon footprint – using the cloud for data storage is much more environmentally friendly than using physical storage devices. Ultimately, it could save your company money on energy bills too.

5. THE DIFFERENCE BETWEEN CLOUD BACKUP AND BUSINESS CONTINUITY/ DISASTER RECOVERY (BCDR)

Cloud backup has been discussed in detail in previous chapters and, in short, it can be described as backing up data to a remote, cloud-based server. As a form of cloud storage, cloud backup data is stored in, and accessible from multiple distributed and connected resources that comprise a cloud.

Conversely, business continuity and disaster recovery are intertwined methods of planning that are integral to ensuring that your business is able to continue operating in the event of a disaster, whether the disaster is human-induced or natural.

Disaster recovery refers to the set of policies put in place to protect your business's technology infrastructure, such as its software or data, while business continuity refers the overall business functions. Both are imperative to ensure that damage is minimized in the wake of an unforeseen event. In fact, a recent study showed that without a disaster recovery plan in place, businesses are likely to go out of business in a period of just 18 months if a disaster strikes.

Simply put, backup, disaster recovery, and business continuity are separated by the time it takes to restore and/or recover your data and get back to work. Business Continuity / Disaster Recovery (BCDR) strategies speed up recovery time from days or weeks to just minutes or hours.

Although the reasons for requiring this type of preventative security are essential, we're taking a closer look at the three main elements contributing to the necessity of BCDR.

It prevents downtime, loss of revenue and potential bankruptcy

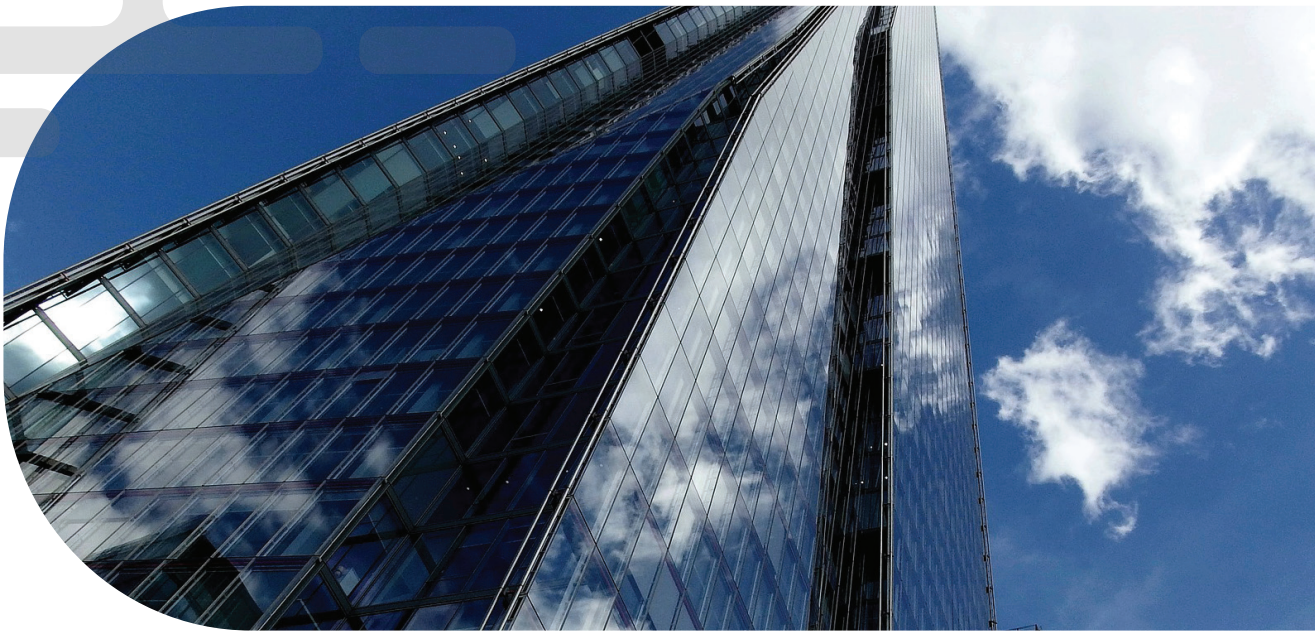
Most businesses cannot afford to have any downtime without it significantly affecting its profits, yet a startling 53% of operations is not equipped to handle even an hour of downtime before they experience a significant loss of revenue. In fact, bankruptcy is a very real possibility when businesses don't resume operations in a timely manner. Having a disaster recovery plan in place ensures that the business will run again as quickly as possible, thereby minimizing any downtime and loss of revenue.

It protects against data loss

A disaster recovery plan will specifically address the ways in which to replicate the businesses' data, which is essential to ensuring that the business can continue to operate. In fact, one study indicated that 87% of businesses that lost access to their data for more than a week were more likely to be out of business only a year later.

It protects your reputation

Unexpected downtime does not only lead to high financial costs, but it can also lead to the loss of reputation due to the fact that customers expect to have access to the business on a 24/7 basis. A disaster recovery plan can prevent reputation loss from happening entirely, or at least minimize the damage.



6. CHOOSING A CLOUD SERVICE PROVIDER

In this final chapter of our article series, we guide you through the process of choosing a cloud service provider.

When choosing a cloud service provider, the reliability and capability of the cloud service provider are crucial. A recent study by IT industry association CompTIA found that very few companies conduct a comprehensive review of their cloud service providers before sealing the deal. According to Tim Herbert, CompTIA VP, “only 29 percent of the companies in the study said they engage in a heavy or comprehensive review of the cloud service providers' security practices”. Understanding your business objectives and how cloud computing services can help you to achieve them, will give you a good idea of the type of service you will require.

Below we list some considerations when choosing a cloud service provider:

6.1 Storage space

Being aware of the storage space offered and the amount of data that can be supported by cloud service providers are always important considerations, as you will often pay for the service cost and not the space you are using. You should therefore know your space requirements beforehand so you can budget accordingly. Additional charges related to the bandwidth, customer support, and software updates, if any, should also be on your checklist.

6.2 Backup frequency

Many businesses underestimate the time it takes to restore normal business operations (the recovery time objective, or RTO) and the cost associated with the downtime to do so. You should choose a cloud service provider that backs up your data at regular intervals (this is referred to as the RPO, or, the amount of time between backups) to ensure your business operations remains intact. You should ensure that your cloud service provider of choice could meet your RTO and RPO needs. When evaluating the services of a potential cloud service provider, “consider whether it offers rapid recovery functionality such as the ability to run operations on the backup server or in the cloud while primary servers are restored.”

6.3 Uptime

Uptime is crucial when, for example, your business runs online and you customers need to obtain information or engagement via your website. If you website experience and outage, it not only affects your business but also your customers. If this is your setup, you need to consider factors such as your potential cloud service provider's uptime history. Do they often experience outages? And, when they do experience an outage, how do they handle it? Some providers commit to 99.9 percent uptime combined with a financial commitment should they fail to be meet the uptime standard. In this regard, your cloud provider's uptime history should guide your decision.

6.4 Security and support

Security and privacy are imperative when it comes to cloud hosting. Your cloud service provider should therefore provide firewalls, antivirus, user authentication, data encryption, security audits and regularly scheduled updates. Not only should your cloud service provider be able to guarantee the security, confidentiality and integrity of your data, it should also ensure that, where applicable, your organisation's industry needs are met.

7. CONCLUSION

This guide provided an in-depth overview of the history of cloud backups, the move away from traditional backup mechanisms and the benefits of backup up data to the cloud. It further aimed to guide you in choosing the best cloud storage and backup provider suited to your specific business needs. Choosing a hosting provider is more than just picking the first one you find. Different needs require different provisions, so be sure to find the right provider for your business.

ABOUT STAGE2DATA

Stage2Data is one of North America's fastest growing and most trusted cloud solution providers. Since 1998 we have delivered 100% Canadian data solutions.

Offering DRaaS as a Hosted service, protecting key servers and data with flexible pricing. 100% Capex and Opex or a Hybrid. Backup Services with the freedom to outsource your data storage needs with confidence and cost efficiency.

As North America's Premier Private Cloud Solution Provider, we provide Cloud Backup services that give you the freedom to outsource your data storage needs with confidence and cost efficiency. Your data will be safe and secure as all Stage2Data backups are protected

For more information on the cloud services offered by Stage2data contact us today.

BIBLIOGRAPHY

i Forbes “State of cloud adoption and security” (23-04-2017) available at https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security/#51e1127c1848.

ii EMC “EMC Global Data Protection Index - Australia Key Findings and Results” (2014) available at https://www.emc.com/collateral/presentation/emc-dpi-key-findings-australia.pdf.

iii Bloomberg “The future of the cloud depends on magnetic tape” (17-10-2018) available at https:// www.bloomberg.com/news/articles/2018-10-17/the-future-of-the-cloud-depends-on-magnetic-tape.

iv Microsoft “What is public cloud” (nd) available at https://azure.microsoft.com/en-us/overview/what-is-a-public-cloud/.

v Webopedia “Cloud backup” (nd) available at https://www.webopedia.com/TERM/C/cloud_backup.html.

vi Stage2Data “The importance of disaster recovery and business continuity” (07-03-2016) available at http://www.stage2data.com/the-importance-of-disaster-recovery-and-business-continuity/

vii Comptia available at https://www.comptia.org/.

viii Carbonite “RTO, RPO and the cost of downtime” (02-10-2018) available at https://www.carbonite.com/blog/article/2018/10/rto-rpo-and-the-cost-of-downtime.