



What to look for in an online backup provider?

Protecting your critical data is an ever increasing concern for businesses globally. Understanding your backup obligations and options makes the choice a little easier. The concept of backing up data has been around for years. As backup evolved with technology advancements, and our reliance on critical information increased, the need for a secure backup method was apparent. For businesses in a competitive environment having their data exposed to threat is not an option. They need to protect it to survive.

Most businesses realise that they need to protect their data and historically methods such as CD's, USB's and manual disks were used. Some companies even took their hard drives home at night! More and more companies' are unfortunately learning the hard way that manual modes of backing up are not the most feasible or cost effective, leaving their companies exposed to data corruption, theft or loss. Hence, the introduction of automated online backup services.

However, as with any other technology, selecting the right online backup solution requires due diligence on your part. Darragh Canavan, Business Development Manager of keepITsafe, has a few pointers to help you make the best decision when it comes to backing up your business data. There's certainly no shortage of providers from which to choose but knowing the right questions to ask can go along way is the selection process.

Below is a list of key topics that are useful to cover when selecting an online backup partner.

Monitoring

When considering an online backup provider you should find out if the service provider offers a fully managed and fully monitored solution or do you manage and monitor it yourself. Also be aware that many providers use fully managed as a selling tool but on further inspection the service requires that the customer manages the backups – for example, many solutions on the market are fixed to send an automatic email to customers every day. If the backup has failed the service is relying on the customer to call their service provider and find out what has happened – a reactive service.

Key questions you should ask

Is support available 7 days a week? Many providers do not have the capacity to offer this service but you will find that you are paying the same rates. Choose a company that has plenty of reference sites and that can guarantee a 7 day week service.

How does the service provider monitor backups? Again, is it proactive or reactive? If reactive and the account contact is away or out of the office this can pose a problem, especially in the event of a failed backup. Companies need to seriously consider this element. Online backup providers who offer a fully managed and monitored service will ring you if there is a problem and resolve it straight away.

Where does the onus lie? Will your backup provider send you detailed reports regarding your backup? Many online backup providers do not have the reporting mechanism to automate this process which leaves the end customer with the responsibility of catching backup issues instead of trained engineers. Ask your service provider if they can detect large file deletions, access permission changes. If not, you need to seriously consider an alternative.

When choosing your supplier find out if the service is a truly managed solution. A proactive service is as follows; trained engineers monitor your backup each and every day and if there is a problem, or a backup has not gone through the customer is then notified. The result is twofold – the customer is getting a completely managed and monitored service and their time can be spent on other aspects of their business.

Monitoring the backups and making sure they went through is critical to any continuity programme in an organisation. Companies cannot afford to suffer downtime due to mismanagement of the online backup process. The best possible

scenario for a user is their online backup solution being fully automated and proactive rather than reactive.

Simple and User Friendly

Look for a service that's easy to use, install and maintain. It is crucial that the online backup provider you choose does not eat into the time of employees. Making sure the supplier can offer a fully managed and monitored service is one point to note as staff time managing the solution will not be required. Data backup should not interfere with your daily business routine. Automating the process should be simple and easy to use.

Datacentres

Through online backup all data is transferred via the Internet to secure offsite datacentres. Your critical company information is then vaulted and kept secure 24/7. Datacentres are fully equipped with around the clock security and high tech equipment to safeguard your data from external threats. It also means that access to the datacentres is nil without security access. Security is at the forefront of all datacentres and online backup providers.

When considering your online backup provider you should ask where their datacentres are located. Location of the datacentre will obviously effect the restore time in the event of a server crash or file deletion. It is in your interest to find out firstly where the datacentres are located and secondly if your data is being stored to one or multiple backup sites. It is advisable to stick with an online backup provider who stores all data in multiple Irish datacentres to future proof your data and increase your restore time.

Data retention policy

Online backup providers usually hold onto data for up to 3 months. You may want this extended. It is advisable to ask if an extended time is available and if you will incur any additional costs.

Proven Track Record

Do your research. Get a list of 5 customers from the online backup provider and call them directly to ask all key information. It is always good to get feedback directly from a customer as apposed to the service provider. Find out what their disaster recovery method is. How long does it take to conduct a full restore? Can they guarantee next

day restore? It is also interesting to know about disasters that have happened that they have solved. Using other search tools such as Google etc to find out background information is also a good point of reference.

Service

If you are a business owner who has a deadline and your server goes down at 1am – what happens next? Is there a phone number you can ring for support? This again comes back to the fully managed, fully monitored element. There are many companies who supply online backup but will not support the service outside of office hours. Are there additional services available to you as a customer? Free installation, advise? All of these are tangible benefits that you need to be aware of when choosing your online backup provider.

Encryption

There is a lot of variety out there in terms of your online backup options. Of key importance is the encryption of your data when moving from one location to another. Finding out the strength of the encryption used while transferring and storing data is extremely important. The standard encryption used today is the Advanced Encryption Standard (AES) Encryption Algorithm

Cost

When comparing costs you should also compare value adds of different backup providers. Not only compare the costs of each online backup provider but also compare it to your method of choice that you are currently using eg Tape.

Available and reliable

It may sound obvious, but any online backup service you choose must be up, running and available 24/7. Do not choose a service that is not readily available. This needs to be a guarantee on the part of your service provider. In the event of a disaster or file corruption you need to know that your data is available for restore 100 percent of the time, again, this needs to be a guarantee from your provider. Data protection and backing up is nothing without the ability to restore at the click of a button.

Growing with you

Over time, as companies grow, so too does the amount of data. When choosing your online backup provider make sure they can grow with you. Talk to your service

provider highlighting the data growth over a period of time. There should not be a huge increase in costs and data increases should be catered for seamlessly.

Indemnification

Make sure your provider has adequate professional indemnity; this gives you, the client some type of protection if the provider is negligent. The value of the indemnity should also be checked. keepITsafe offer €1,000,000 per client.