Why you need to include the **Cloud** in your **Disaster Recovery Plan**

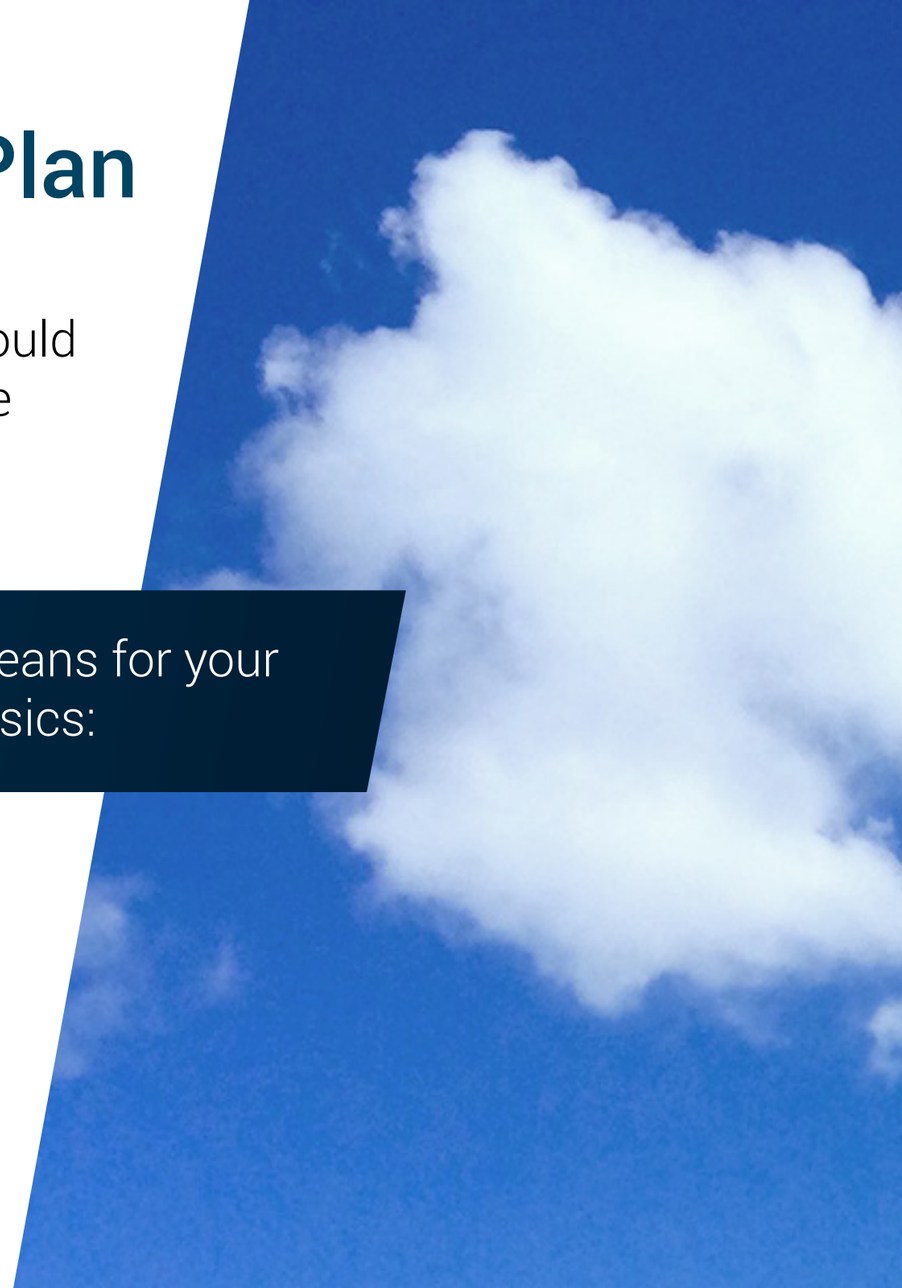
StorageCraft

The **Cloud** and your **Disaster Recovery Plan**

We are bombarded with information and articles on why companies should back up data to the cloud and how cloud-based Disaster Recovery is the only way forward for companies to truly protect their data.

There is a lot of information, questions and advice on what the Cloud means for your business, all of which which can be confusing, so let's go back to the basics:

- Why do you need to back up?
- What is backup vs Disaster Recovery?
- Where does the Cloud fit in?
- Are all Clouds equal?



Data is the lifeline of your business

All companies need to protect themselves against data loss and downtime which can happen as a result of human error, hardware failure, software corruption, natural disasters, ransomware,… In IT circles we often say ***"it's not a case of if disaster happens, but when disaster will happen"***.

Based on findings of the Aberdeen Group, downtime that lasts for one hour can cost small companies as much as £6,500. Mid-size companies will lose around £60,000 per hour and large enterprises over £563,000 for an hour of downtime*. Further research shows that 90% of companies losing data from a disaster are forced to shut down within 2 years.

** Prices have been converted from Dollars to Sterling*

Statistics show that 65% of companies have no backup or recovery plan. Many companies today do not equate their data to being their business. Are you one of these companies?

Most companies would agree that some form of contingency plan is needed to ensure they do not lose precious data and suffer long periods of downtime. Contingency plans to deal with disasters and downtime come in all shapes and forms and you can expect to hear such terms as Backup, Disaster Recovery (DR) and the Cloud being used.

Backup is not equal to Disaster Recovery:

Understandably many people don't grasp the difference between Backup and Disaster Recovery. Yet the distinction is crucial and will be a key factor in ensuring your business will be back up and running with minimum interruption when any form of outage/disaster happens.

Let's be clear that disasters come in all shapes and forms and, all too often, companies need to protect themselves from their own errors and mistakes.

What about the employee that forgets his laptop, containing critical files which have not been backed up, on a train, plane, …?
What about the CEO that deletes his Office 365 file with no way of retrieving it?
The list goes on…

Broken down to its simplest, a DR solution is what enables you to restore quickly and efficiently when needed. Being able to back up is only one part of the equation and while ensuring that you take clean, regular backups of all your systems is essential, it is of little use if you are unable to restore from these backups. Therein lies the difference between a backup and DR solution.

So where does the Cloud fit in?

Let's take a quick look at basic
Disaster Recovery Best Practices
to see where the Cloud fits in:

1. Local Backup

The 1st step is to start with a local backup which means exactly what it suggests: ensure you back up your data and systems on your local site.

In the vast majority of cases you will restore from these onsite backups.

2. Replicate Offsite

This 2nd step eliminates the notion of a "single point of failure". Put simply, if something goes wrong with your local backups, you cannot access your local site, your office is flooded, … you need to ensure that you have sent a copy of your backup images offsite. This is where the Cloud discussion starts…

Offsite

You may decide to replicate copies of your backup images to another office, to your service provider's office or you may replicate your backups to the Cloud (data centre shelf space owned by you, your service provider, DR vendor or you may work with a public cloud provider):

In the spirit of keeping things simple we are going to break Cloud offerings into 2 categories:

1

At its most basic the Cloud is a data centre where your backup images are replicated to.

A. In simple terms, the Cloud is where you store your data. Being able to quickly restore data in this scenario may be difficult. You will, most likely, have to factor in a number of days or weeks to get data back.

B. You will, most likely, have to contact your service provider and/or Cloud provider to restore data, the notion of self-service restore will most likely not apply here.

C. You may have to pay fees (on top of storage fees) to access and restore your data.

Offsite (continued...)

2

At its most sophisticated the Cloud is where you can spin up and run your business from, in 1 click, when you cannot access your local backups.

A. In simple terms, the Cloud is, in fact, a purpose-built Disaster Recovery data centre from which you can run your business, while you resolve your onsite issues.

B. You can spin up your entire network in minutes. You can literally flip a switch and failover to a secondary network running in the cloud in just minutes.

C. With the necessary expertise onsite, you can take complete control of the restore process and spin up your infrastructure directly without contacting or waiting for your vendor or service provider.

D. Typically, purpose-built DR Cloud offerings will offer multiple recovery options including: drive based recovery, file and folder recovery or full virtualization of systems in the cloud.

Which Cloud to choose?

Choosing the best Cloud for you means asking yourself the following questions:

Do you work in a regulated industry of any kind?
If the answer is yes, then you will need to ensure and demonstrate that your business can operate in all scenarios and that you have the best solution in place to ensure that downtime is reduced to a strict minimum. The ability, not only to restore, but also to vigorously test restoring from the Cloud, will be necessary in this case.

What are your Recovery Time Objectives (RTO)?
Put simply, how quickly do you need to be back up and running following a disaster? If you have tight RTOs you need to ensure that you can run your business from the cloud and be operating in minutes following on from any disaster.

What are your Recovery Point Objectives (RPO)?
Put simply, how much data can you afford to lose following a disaster? Ideally your Cloud offering will allow you tailor your service levels and recovery options to the data in question: in some cases, restore via a hard drive may be sufficient but for your mission-critical data you need to be sure you can virtualise in the cloud easily and quickly.

Where is the data stored?
You may need to ensure that data is stored within a specified geographic region. Make sure that the data centre meets the minimum data centre requirements necessary for your business and that Advanced Encryption Standard (AES) is being used when your data is being transferred to and from the cloud.

In Conclusion

Your company's data is your most valuable asset. It's not an overstatement to say that without your data, you have no business. Having a robust, tried and tested Disaster Recovery plan is an absolute must for companies of all sizes. Regular backups are the foundation stone of your DR plan.

You must understand, however, that these backups have no value if you cannot restore quickly and easily when you are hit by hardware failure, a ransomware attack or any of the many waiting-to-happen disasters looming. Fully protecting your business involves getting copies of these backups offsite, and one great option is to replicate to a purpose-built Disaster Recovery Cloud allowing you to literally flip a switch and failover to a secondary network running in the cloud in just minutes.

Interested in finding out more about the **StorageCraft Recovery Solution** and **StorageCraft Cloud Services** **click here >>**

StorageCraft.