Technology Risk Management: Data recovery in a cloud computing environment

The IT Psychiatrist
Keeping your tech in check

In moving their data to the cloud many companies are inadvertently exposing themselves to the risk of data loss. Without proper controls in place data can be lost through user error and synchronisation issues, or more malicious activity such as hacking or a disgruntled employee. Unless a managed back-up plan exists the data may be lost forever. This paper explores the risk of data loss in the cloud, provides cases studies into protecting from data loss, and closes with tips for ensuring data is recoverable.

What is cloud computing

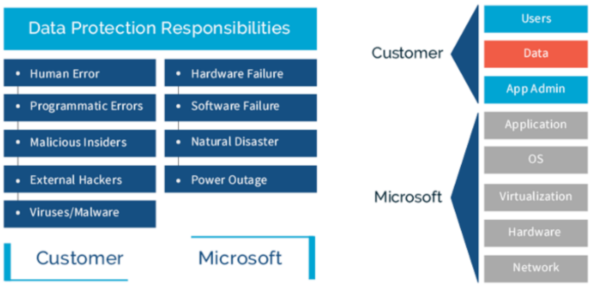
Cloud computing is the practice of using a network of remote servers accessed via the Internet to store, manage, and process data, rather than a local server or a personal computer. Common examples include Office 365, Google G-Suite, and Xero. The cloud has many benefits including affordable prices, access to massive storage, and remote accessibility, but it is not 100% fool proof.

Many cloud service providers market their services on the benefit of the availability of data – by using their tool, all data is retained and accessible. While this is accurate, most cloud tools are quite clear in their terms of licence that they will not guarantee availability of data in some specific scenarios. Even if you trust the most reliable cloud services with your data, things can go awry at any point and a loss may permanently destroy critical information.

1/3 of businesses have experienced permanent loss of data that is stored in the cloud.

So, who is responsible for your business data?

The main business model of cloud computing is a vendor will look after all the data you want, but they will not be responsible if it is deleted by you.



The associated graphic shows the responsibilities of data management in Office 365 but is indicative of many agreements in place with vendors. While Microsoft are responsible for some scenarios, several obligations fall on the customer.

What they do not cover falls into two categories:

- **Active Deletion** - The customer has an active subscription and a user deletes data, or data provided by a user is deleted by the administrator. This could be accidental or more sinister.
- **Passive Deletion** - The customer subscription ends. This is usually where a staff member leaves the company but can be where a company opts to change tools.

Case Study 1: Incorrect syncing

Working in the health industry means that medical centres are heavily regulated, and compliance is particularly important.

A local clinic's data loss problems began when an HR folder stored in Dropbox was moved. Unfortunately, the synchronisation did not work correctly. As a result, all files disappeared – including many that were not even owned by the staff member moving the folder. The employee checked the trash bin, recycle bin, and desktop for a copy – but the data was gone.

In this instance the clinic opted to use Dropbox because it was free. They had no support setting it up. As a result, there was no backup in place and no-way to recover the data.

Technology Risk Management: Data recovery in a cloud computing environment

Deleting data can mean it is gone forever

In many instances, the vendor will keep data that is deleted by a customer for a short period of time, typically 30 days, but will eventually delete it. It is also possible that the data can be purged by the user early, a possible avenue from a malicious attack. Once that retention period ends there is no way of recovering data that has been deleted.

This could cause issues further down the track, especially when it comes to regulatory obligations or customer disputes.

It is possible to prevent this data loss with the appropriate controls in place.

> *Case Study 2: Tidy kiwis*
>
> Charity organisations do so much with minimal resources, but like any organisation must deal with staff turnover.
>
> A national charity came unstuck when a departing employee took the time to clean up some of the emails that were stored in Office 365 before they finished. Their motivation behind this is unclear, but the consequences where severe as amongst the deleted emails were messages that were critical to a major fundraising initiative.
>
> Losing this kind of data within any organisation can have catastrophic consequences, and it ran the risk of setting back the fundraising activity by months.
>
> Fortunately, the charity was working with a local IT company who had ensured that adequate backups were in place. The lost emails were able to be recovered quickly and the fundraising went ahead without issue.

How you can protect your business

Cloud data storage has worked well for so long that it is natural to assume that everything is safe. While it is impossible to protect against everything, following these steps will minimise the chances of cloud data loss

1. **Know your obligations** Do not leave it to chance, ensure you understand what you are responsible for when signing up to use a cloud service.
2. **Backup to other sources** Do not store everything in the cloud if you want to give yourself a good chance to restore data when failures and outages occur. There are many services available which make it easy to backup critical data even if it is primarily stored in the cloud.
3. **Make sure your security is up to date** Weak security systems can leave your systems vulnerable to malicious parties. Make sure your security is up to date and working.
4. **Ensure you have the right policies in place** Having the right rules and guidelines for managing, operating and using the organisation's information systems are critical to ensuring your data is protected

Unsure on the risk on your business for data stored in the cloud?
Contact us today for a free assessment.

We might save your business.