What if something happens to your backups?

By Iniel Dreyer

25 Oct 2021

Data backups are essential. Most businesses are aware of this, and many keep a second and even third copy of their data in a different location. The issue is that this secondary location is often in the same vicinity as the primary data source. But what if something happens to your data centre? What if you are physically unable to access your data due to external factors like a Covid-19 lockdown or rioting? Keeping backup data at the same location as primary data is a risk to business. Offsite data backup has become essential to help businesses safeguard data against loss and be able to recover in the face of a range of different challenges.

Iniel Dreyer, MD at DMPSA

Threats outside of business control

Having backup data is vital in helping businesses to recover lost information if it is accidentally deleted, or if a ransomware attack occurs, or any number of other problems that may result in data loss. However, a business could have the best quality backup in the world, and still fail to achieve business continuity, because external factors must also be considered. The recent rioting in South Africa threw the need for offsite backup into stark relief.

What if your business had been looted or burned down, taking with it not only the production database but also any and all backups stored onsite? What if data was being backed up offsite to a data centre, and the data centre was looted or burned down? What if backup strategy requires someone to physically retrieve a copy of data in the event of a loss, and nobody is able to get to the data because riots have shut down the roads, or Covid-19 has caused another hard lockdown? The risk of maintaining backup and production data at the same location is untenable for business today, and backup strategy needs to be reconsidered.

Best practices

The reality is that if data is lost and is unrecoverable, many businesses will be unable to recover from the loss. Equipment can be replaced, even though this may be a costly exercise, but once data is gone, it cannot be returned without a working and available backup. It is imperative to keep data offsite, not only in a different room in the same building, but at a completely different location, which is at least 50km away, according to data protection best practice.

The cloud has made this even easier, as data can potentially be stored anywhere, even in another country should data sovereignty allow for this. However, this is a challenge that many businesses continue to grapple with. The recoverability of data must be weighed against the requirements of compliance regulation, and the context of the data needs to be understood. A trusted service provider can assist businesses to find the right solution and the right balance to meet their requirements.

The bigger picture

It has become critical to look at the entire picture of data, including its context, in order to find the most suitable solution for data backup. The underlying requirement is that a reliable copy of data should be stored elsewhere, offsite, but the type of storage should be based on the data itself and how it needs to be accessed.

Data must be classified to understand its value and importance to the business, which will in turn govern the way it needs to be stored. For example, historical patient information must be retained for compliance purposes, but may not necessarily need to be accessible instantly, whereas live financial information is far more time sensitive.

There is no ‘one size fits all’ approach to offsite data protection, and every method of storage will have cost and performance implications for the business. Working with a trusted service provider will help businesses to understand the importance of various types of data, which in turn will define where and how it is stored, the cost of this and how quickly it can be recovered.

Data loss versus disaster

There is a vast difference between recovering a file that has been deleted, and recovering from a total system failure or unavailability. Complete disaster recovery involves so much more than just data backup and recovery. Context is always important, because not all data is the same, which means that having an entire system replicated on hot standby is often an expensive and unnecessary approach.

Not all data is created equal, it must be classified according to the repercussions to business should it become unavailable, and this needs to be aligned with the greater business continuity plan. Ultimately, data backup is an insurance policy - you need to make sure you are not over- or under-insured, that you are only paying for what you need, and that you are covered in the event of a disaster.

ABOUT THE AUTHOR

Iniel Dreyer is the MD at DMPSA