BIZCOMMUNITY

Data Backups: Start with what you can't afford to lose

By Chris de Bruyn

16 Sep 2019

Toy Story 2 almost didn't happen. Somewhere during the 3D animated movie's production, an administrator accidentally destroyed all of the movie's data assets, including the meticulously crafted models and animations. Were it not for the technical director, who made backups to continue her work at home, Pixar's ground-breaking sequel may have never come to life.

Chris de Bruyn, Operations Director at Gabsten Technologies

This happened 20 years ago. Today, it would be impossible to store such a project on even a handful of external drives. The volume of data is much greater and modern environments more complex: what about applications, operating systems, virtual machines or configurations? Do you have plans for those?

Saving everything isn't a strategy. It's the single biggest mistake companies make around backups (apart from having no backups!). This can cause large yet avoidable costs due to the fact that not all data needs to be stored in the same way. However, even 'everything' is a subjective scope since people often don't know what should be backed up.

You can use a simple rule to clear this up: if the data is critical to your business, if your business could stall and close its doors when something happened to that data - then it's critical data.

Defining critical data

Yet, this definition of critical data is unique to your operations. Its behaviour (how it is accessed and used) drives your business continuity strategy. Some data might need to be on-site for quick recovery, but for other uses – perhaps a roaming sales force - a cloud-backup system could be much more convenient. You may only need to save production files because reinstalling operating systems and applications is quick. But then again maybe there are carefully managed and delicate systems that will take much less time to recover than recreate.

Therefore, poll everyone on what data they use and how they use it. Backups should meet the requirements of tax legislation or privacy laws such as GDPR and POPI Act, however, effective data backups start at the operational layers – and it's the people at the coalface who can give the best practical insight.

Assume nothing, even at the technical levels. Your systems may have been installed by an engineer who has since left the organisation but, does their replacement have sufficient understanding of the system requirements to recover those successfully? It's important to explore such questions without judgement. Data planning requires collaboration to avoid disastrous loss and finger-pointing later.

Understand your data

Moreover, an Enterprise Content Management (ECM) service is a useful way to start understanding your data and recognising what is critical. This can identify important data, encourage employees to recognise such data and their relevant ownership, and drive policies for data backups. You can also establish an internal committee using different people in the organisation to guide business continuity efforts.

In addition, remember that data backups are not optional. Every company must have a Disaster Recovery or Business Continuity strategy, tested often - monthly, if possible. Yet, throwing all your data into one backup pool is pointless and expensive. Good backups depend on you knowing your data and its behaviour. Your business strategy must reflect the understanding of what data keeps your organisation breathing.

You might be lucky and an employee diligently copied files out of harm's reach. But this isn't 1999. Today data is everywhere, from information to applications. If you want to keep it safe, start by knowing what data is needed to keep everything going.

ABOUT THE AUTHOR

Chris de Bruyn, Operations Director at Gabsten Technologies