What businesses need to know about business continuity, disaster recovery

By Mike Rees

15 Nov 2018

The smallest disruption to a business can have a long-lasting impact, from interrupted production to lost customers. It's critical that businesses have a business continuity plan in place to not only minimise the impact and recover from any incident which can negatively impact operations, but also to minimise the duration of any interruption and continue with business as usual - wherever possible.

Mike Rees is territory account manager for South Africa, Commvault.

Business continuity vs. disaster recovery

Data is seen as the crux of most businesses; therefore, many assume accessing, protecting, backing-up and recovering data is all that is needed for business continuity. As such, the business continuity plan is left to the IT department – in its entirety. However, business continuity should not be confused with Disaster Recovery (DR) and extends well beyond the realm of IT's control.

DR has to do with data protection and recovery, as well as how quickly a business can regain use of their business-critical technology and systems in the event of a disaster. Disasters are seen as any event or incident which inhibits access to – and use of – business technology or systems, and ranges from loss of power to cyber-attack to physical events such as a fire.

Study shows people and organisations don't fully trust anyone with their online data

13 Nov 2018

Business Continuity (BC) has a different function and covers the policies, tools and procedures a business needs to have in place to ensure that the entire business can continue as normal in the event of a disaster. This includes aspects such as ensuring staff can work even if they cannot access the physical premises, or that customers are given the same level of service they expect even if there is a power outage, for example.

DR forms part of the BC plan and IT should be included in formulating the BC plan. Nevertheless, the entire business should be involved in establishing what the priorities are and how to ensure they are maintained.

Why do you need it?

Disaster can strike at any time. In South Africa, we have particular challenges such as unreliable power supply and insufficient bandwidth coverage and speed. The likes of cable theft affect both and can leave a business unable to function properly.

Organisations are also faced with a growing risk of cybercrime, which is impacting more and more businesses as we grow more connected.

Avoid following a tick-box approach in your DDoS defences

12 Nov 2018

Business continuity strategy give businesses direction and a plan to follow in the event of these, or other, disasters happening, ensuring that businesses do not suffer the impacts of interrupted operations, dissatisfied or lost customers, and – ever more importantly – lost and irretrievable data.

What's available

Luckily for businesses, many outsource companies offer disaster recovery as well as business continuity as a service.

Technology certainly does provide many solutions for both DR and BC, however, BC solutions used to incorporate temporary physical working premises, the advent of smart devices and cloud-based applications means that most employees with access to the Internet can perform their jobs from anywhere, in the event of being unable to access the office.

Most data storage and management solutions, today, are cloud-based, offering both the redundancy a business needs as well as the accessibility – staff can access the data from anywhere, provided they have the right permissions.

Then again, no solution is effective without building and implementing a BC and DR strategy, or plan. This needs to include the relevant frameworks, governance policies, processes, and tools to effectively identify which business applications, systems, and tools are most critical and prioritise their recovery to continue running. And don't just formulate a DR or BC plan, test it regularly and revise it appropriately, then test it again.

What to remember

Businesses cannot afford to simply be reactive to disasters, they need to ensure they have the right security mechanisms and safety methods in place to proactively prevent disasters, too. This should include security, data protection and redundancy.

A business can have the best-laid plan in place, however, if it's not tested regularly, it can backfire and fail when its needed most. Both BC and DR plans need to be regularly tested through active simulations to ensure that nothing is missed. Priorities change; compliance requirements evolve, and businesses grow – today's plan may not be effective tomorrow.

With regards to disaster recovery, businesses need to ensure the solution they opt for is resilient. It needs to not only offer data back up and protection, but also availability and easy recovery. To ensure this, data should be prioritised, bearing in mind that not all data is equal. Businesses should ensure they know what data they need and use regularly, versus the data that is less important and may not impact operations or customer service delivery.

ABOUT MIKE REES

Territory Account Manager: South Africa at Commvault

- Consolidating your backup and recovery makes sound business sense - 21 May 2019
- Optimising data storage has many business benefits - 22 Feb 2019
- Data governance is not just about compliance; it's good business - 10 Jan 2019
- What businesses need to know about business continuity, disaster recovery - 15 Nov 2018
- Ransomware is here to stay - can your data say the same? - 23 Nov 2017

View my profile and articles...