BIZCOMMUNITY

Achieving business agility by planning for the worst

By Kate Mollett

28 Mar 2019

Business agility has become a critical enabler in today's digital environment. According to Forrester, it is one of the best ways to secure a long-term competitive advantage in a globalised marketplace. And yet, outages can take it away with one snap of the fingers. They wreak havoc on a suffering company's critical services, and at a time when customer expectations are skyrocketing, cause significant reputational damage which can take years to repair.

Kate Mollett, regional manager for Africa at Veeam

In an age governed by information and the ability to access it, unfortunate incidents like those suffered by Liberty Holdings, ViewFines, and even Facebook last year are a pertinent reminder of why businesses can ill afford their lights to go out. The ability to remain 'always on' is crucial.

But this is a challenge that is far from simple to solve.

Given the widespread use of third-party cloud providers, guaranteeing availability is not just a case of a company having its own resilient backup and recovery options in place. Companies must be able to trust that their third-party providers are following suit. After all, what would be the point of keeping everything in working order if your staff or customers still cannot access the services they need? Thousands of companies have little or no IT staff to depend on and are almost entirely reliant on external service providers to deliver what they need to meet their agility goal.

Risky business

However, despite pressure to maintain this level of high-speed functionality on behalf of their customers, major cloud providers continue to struggle with regular periods of downtime and disruption when trying to maintain service levels. These are choppy waters. The knock-on effect of such incidents can be extremely costly; our 2017 research showed the average cost of downtime globally for mission-critical applications can rise to more than R1m per hour. The average annual cost of downtime sits at more than R301m, which is not something that many companies can survive.

How can businesses mitigate against such a costly risk?

The best way to ensure survival is by being prepared. Whether a business needs to watch its own back or has a responsibility to the ongoing success of others, having a plan in place to follow if an outage occurs (that can help recover and get back online quickly) is key. The IDC estimates that 80% of businesses that do not have what is defined as a 'disaster recovery plan' in place will simply fail when an outage strikes, not to mention suffer an almost incalculable drop in revenue resulting from falling customer trust.

Putting plans in place

So, what does a disaster recovery plan look like?

Businesses can start their preparations by first ensuring they understand where disaster recovery sits within the context of their overarching business strategy. This is where an impact assessment comes in. Businesses need to take the time to identify which apps and businesses processes are critical to daily operations.

They must calculate the maximum amount of downtime they can stand for each of these before they fail. Factors like these make it possible to calculate the ideal recovery targets for these apps and processes. Additionally, it enables them to appropriately identify what measures are required to meet these requirements.

The choice of partner to help implement an effective disaster recovery plan is also a big decision. Factors such as the experience of the partner and the nature of the service level agreement (SLA) that they offer are critical. Elements like uptime guarantees, turnaround time on service requests and enquiries, as well as fees and compensation, should all be part of even the most bare-bones SLA. With the continued push on businesses to be always-on, these will only become more important considerations.

Compliance is also a factor that should not be taken lightly, and any service provider worth taking seriously will be fully compliant with the legal requirements of the territories where they operate. This is especially the case for local businesses who need to remain cognisant of the Protection of Personal Information Act as well as the General Data Protection Regulation of the European Union if they do business with member states.

Storage location

Location is as important a part of the process as the planning stage. Choosing on-premises or an offsite location for data storage can make a real difference to any given company's ability to react, with each having their own strengths and weaknesses. A 3-2-1 strategy is one of the most popular choices we see businesses make, which involves keeping three copies of data on two different types of media, with one being offsite.

Offsite data centres can be often more convenient and reliable, as optimal conditions for your servers and equipment are always maintained, and tech support and security are always on hand. If plans include significant expansion using the

cloud, having access to offsite capability that can be quickly scaled up may also be important. However, having critical data physically separated in this way suddenly places greater priority on strong network access, so extra or more reliable bandwidth might be needed. We also return to the issue of whether the offsite provider can be trusted, as we need to remember they too have their own challenges to maintain service and foster their own business agility.

Recently, South Africa saw the launch of two Microsoft Azure multi-national data centres providing businesses of all sizes with a cost-effective, reliable, and fast alternative to international options. Again, the same principles must apply. Ensure adequate backups are in place, SLAs are adhered to, and business continuity remain the focus.

Uncertain times

Planning for the worst by taking all these elements into consideration can make a massive difference when it comes to mitigating the threat of outages and downtime. However, a disaster recovery plan on its own is still not enough. Businesses need to be regularly testing the viability and quality of their backups to be certain they are completely recoverable and dependable. The worst time to learn that the backup procedure has not been working properly is when they are the only option.

Economic and political climates remain uncertain, but what is crystal clear is that industry competition has become fiercer than ever. Agility has therefore never been more important, reflecting how it can become a powerful competitive differentiator. But this ability to act quickly can disappear equally as fast, resulting in catastrophic consequences. Businesses face huge pressure to ensure their services never falter and remain highly responsive. They cannot afford to grind to a halt. Planning for the worst is imperative, recovery is key. This is how businesses achieve and maintain their need for speed.

ABOUT KATE MOLLETT

Kate Mollett is senior regional director at Commvault, Africa South and East.

- Modern data challenges demand advanced management platforms - 4 May 2023
- #BizTrends2023: The major trends to impact the data landscape in 2023 - 9 Jan 2023
- Ransomware is a business resilience issue, not an IT problem - 16 Sep 2022
- Big spike in ransomware attacks calls for adoption of backup-as-a-service - 14 Apr 2021
- Successfully managing risk in a digital world - 3 Jul 2019

View my profile and articles...