COMMVAULT

WHITEPAPER

Disaster Recovery waits for no one

Improve backup and restore performance, while lowering data management costs and overhead.

It used to be that all you needed your Disaster Recovery (DR) strategy to worry about were tornadoes, floods, power outages, and the occasional monster attack. These days disasters have taken on new and more subtle forms thanks to the increase in malware and ransomware. These types of disaster are harder to detect, and much more complicated to respond to. So, how can you make sure you're DR plan is ready?

No matter the disaster – whether natural or man-made – you need to respond quickly. But you shouldn't have to break the bank being ready for faster restores and better data availability. With these four data-recovery best practices we'll help you make sure your environment is ready for when disaster strikes, and even save some cash along the way.

Downtime can be expensive, and the costs to the business are not only dollar amounts, but factors of lost productivity and time. If your internal and/or external customers are unable to access your services, the impact to your business can be significant.

$26.5 billion cost of lost revenue in North America due to downtime[1]

So, what can you do that actually will help you avoid being the next headline? Well, let's take a look at how you can ensure your IT services are ready for action, and the data can be quickly put back where you need it to be.

1 Hit your backup targets

Sure, there are a lot of ways to make sure your data is protected, and some of those can be pretty expensive to implement (looking at you "real-time replication"!). Not every application or workload needs that extreme level of availability. Knowing what data you have will help you set your priorities, and properly align each data set with the appropriate protection method. Regardless, all of them will at least need some form of backup or you won't have anything to recover from. Having the ability to provide flexible options and tiers for protection and knowing what data falls into which will help you line up your SLAs with the business needs without overspending. Work with your business owners, understand their needs, and put in place the solutions to hit those targets. Not everything needs "Five 9's" protection, don't pay a premium for things that don't need it.

5 ways to get control of your backup and recovery environment. Read >

2 Don't forget about the cloud

Flexibility is the key here. It used to be you needed to have identical hardware sitting idle "just in case," but you don't need to do that anymore. The cloud is an excellent target for Disaster Recovery. The ability to quickly deploy storage and compute when needed, and then turn it all off again when you're done is a cost effective way to run Disaster Recovery. Being able to restore your data somewhere else is important because the original location might be unavailable, or not trustworthy (think ransomware). Having the option of taking your data and recovering it to the cloud, or several clouds, should be included in any updated Disaster Recovery plans.

1 Hashedout, 80 Eye-opening Cyber security statistics for 2019

3 Everything's automatic?

If your Disaster Recovery plan includes the step "Janet pushes the red button," you might be in trouble. The more you must rely on manual intervention, the more likely you are going to run into delays or failures in your recovery efforts. Wherever possible, try to ensure that tasks, such as failover, are automated with the appropriate checks and balances to ensure that each stage of the recovery is progressing as expected. This should be a "no-brainer," but far too often organizations are still relying on people to drive their plans forward. If those people are unavailable or cannot get to where they need to be, you need that automation to execute your recovery plans regardless. Being able to coordinate provisioning of resources and then bringing your workloads online within the cloud is the perfect use case for automation and rapid recovery.

"If you're not able to recover, that's kind of a resume generating event."

Commvault Customer Champion Alliant Credit Union | Data Protection Solutions for Banking

4 Eliminate data silos

If you don't have an easy way to see, move, and recover your data, you're at a disadvantage when it comes to Disaster Recovery efforts. Often, solutions have been built with pieces of different tools used to solve different problems. This overlapping, and redundant approach just brings more headaches to recovery as you must go into multiple places to bring different data sets back online. You need to look for solutions that will deliver a single view of your data across your entire environment – no matter what that data is or where it lives. Having native API integration across your applications, databases, hypervisors, cloud platforms and storage arrays will mean less complex custom scripting (human error), more automation, and ultimately faster recovery.

These days, disasters come in all sizes and shapes, and your Disaster Recovery plans need to be able to respond quickly to whatever problems arise. Plan for them with solid data protection, using automation, extending to the cloud, and simplifying your IT environment with a solution that can cover all your data, not just pieces of it.

Using these strategies your data will be ready for when disaster strikes.

commvault.com | 888.746.3849
get-info@commvault.com