COMMVAULT®

▶ 5 Benefits of Disaster Recovery in the Cloud.

One of the biggest use cases for the cloud – in fact, the biggest, in the case of hosted private cloud – is for backup and disaster recovery. It adds up to one thing: Organizations are counting on the cloud to make sure they retain access to their critical corporate data.

Companies are putting their money where their mouth is, too: Forrester estimates in 2015, companies will spend over $90 billion on cloud services.[1] Specifically, IDC estimates that backup-as-a-service and recover-as-a-service will account for $1.023 billion by 2018.[2] And Gartner predicts that by 2020, 90% of disaster recovery (DR) operations will run in the cloud.[3]

As the cloud has become more accepted, an increasing number of organizations have been putting their data into the cloud. But for the cloud to become a useful repository for disaster recovery, that means that organizations need to be able to get their data out as well.

1 Forrester, "The Public Cloud Market Is Now In Hypergrowth," April 2014
2 IDC, "Leveraging the Public Cloud for Faster Disaster Recovery at Lower Cost," May 2015
3 Gartner Symposium

INCREASED INTEREST IN DISASTER RECOVERY

It all starts with organizations realizing how important disaster recovery is. Until recently, disaster recovery didn't get the attention it deserved from businesses because of the cost and complexity of doing it right. Moreover, business units didn't see a direct benefit from disaster recovery — until a disaster occurred.

IDC estimates that as many as 50% of organizations have inadequate disaster recovery plans. In fact, IDC warns, such companies might not survive as a going concern after a significant disaster because of their inability to recover IT systems.

"In many cases, IT managers may have only a vague idea of how they would reestablish application services, lack up-to-date runbooks, and have no contingent personnel plan," IDC writes. "Disasters do happen and not always to the other guy." But as many as two-thirds of organizations don't have any disaster recovery strategy at all, warns the 451 Group[4].

Until the cloud, most disaster recovery scenarios involved significant costs to guard against a relatively rare occurrence – a scenario that led to too many organizations not giving disaster recovery the attention that it deserved.

"While a DR budget from IT may be submitted annually to management, it always seems to be the first thing dropped from the overall budget as soon as constraints are applied," IDC writes. "Management often experiences sticker shock at the cost of DR for something perceived as a remote possibility."

What's worse, though, is that individual business units might not be aware that the company doesn't have a disaster recovery plan, simply blithely assuming that operations would be restored promptly after a disaster.

The best way to persuade management to spend the money it takes to do disaster recovery right? Figure out how much it would cost not to have it. IDC research indicates that the average cost of downtime is about $100,000 per hour, although it can go as high as $1.6 million per hour for some organizations. And recovery from a true disaster could take several days or even weeks without adequate planning.

In fact, IDC also found that most organizations experienced between 10 hours and 20 hours of unplanned downtime per year, even without a disaster. The good news? An average organization could spend between $1 million and $2 million on a contingency system and still achieve a one-year return on its investment, just by eliminating that downtime.

Best of all, with the emergence of cloud computing, there are now full-blown disaster recovery solutions available to small, medium-sized, and large businesses alike that help companies reduce costs without sacrificing service.

SUGGESTED READING >>

IDC Whitepaper: Leveraging the Public Cloud for Faster Disaster Recovery at Lower Cost[i]

Read how cloud computing can be leveraged to develop DR capabilities that are both less expensive and easier to deploy than traditional methodologies.

READ NOW

PDF

What is it about the cloud that makes it so well suited for disaster recovery?

CONSERVING RESOURCES

Organizations using the cloud for disaster recovery don't have to go to the expense of setting up a duplicate data center – not to mention, one that sits idle most of the time, waiting for a disaster. Companies that do decide to go this route can either set up the duplicate data center on their own, or through a specialized third-party datacenter or co-location facility that hosts multiple subscribers.

While the third-party approach means the organization isn't responsible for maintaining the second data center, it also means the systems may be shared with other organizations in the event of a regional disaster. Other disadvantages are that it can be difficult to maintain hardware compatibility.

But using cloud-based disaster recovery is even more attractive economically because it doesn't require a huge up-front capital investment.

FASTER RESPONSE

Using the cloud also means that organizations can respond more quickly to a disaster, sometimes in as little as a matter of minutes. In fact, companies can actually recover from a disaster within the cloud itself, using cloud orchestration and automation tools to automate the in-cloud recovery process from end to end.

Without such automated tools, recovering from a disaster means scripts, as well as manual administration and intervention – all of which means that IT can't meet critical recovery service level agreements. When a true disaster occurs, many businesses may find implementing their disaster recovery solution takes longer than they expected – at best. At worst, organizations may find that their data is not recoverable in the way they thought.

Recovering from a disaster within the cloud also means that organizations don't need to take the time, processing, and cost associated with recovering everything from the cloud to on-premises. That way, recovery can be limited to critical data, further reducing costs.

"The average cost of downtime is about $100,000 per hour, although it can go as high as $1.6 million per hour for some organizations."[5]

IDC Technology Spotlight, May 2015

MORE FLEXIBLE

Finally, organizations that choose the cloud for their disaster recovery solution don't have to pick a location for a disaster recovery facility

5 IDC Technology Spotlight, Leveraging the Public Cloud for Faster Disaster Recovery at Lower Cost, May 2015

and cross their fingers hoping that it, too, doesn't end up stricken by a disaster. Many companies struck by Hurricane Sandy in 2012, or even thunderstorms that same year, found that their disaster recovery facilities were in the path of the same storm. With the cloud, disaster recovery facilities can quickly and easily be moved to different parts of the world.

Moreover, because of the way the cloud works, a company needs to reserve – and pay for – only the amount of data it needs and is actively using. Business units can decide exactly which data is the most critical to recover, reducing costs just at the time when the organization most needs economy.

All that said, even with the cloud, an organization can't just set up a disaster recovery plan and walk away. Disaster recovery plans should be tested at least every year, and quarterly is even better, warns IDC, adding that products that can simulate tests and do pretest checks are particularly helpful.

"Management often experiences sticker shock at the cost of DR for something perceived as a remote possibility."

IDC, "Leveraging the Public Cloud for Faster Disaster Recovery at Lower Cost," May 2015

RESOURCES

i commvault.com/resource-library/555d8b0d00e072a74700007f/idc-report-leveraging-the-public-cloud-for-faster-disaster-recovery-at-lower-cost.pdf

To learn more about Cloud Disaster Recovery with Commvault® software, visit
commvault.com/cloud.

COMMVAULT®

PROTECT. ACCESS. COMPLY. SHARE.

Commvault.com | 888.746.3849 | get-info@Commvault.com
© 2015 Commvault Systems, Inc. All rights reserved.