REPORT REPRINT

Disaster recovery preparedness gaps highlight future vulnerabilities

APRIL 15 2020

By Henry Baltazar

Although disaster recovery continues to be a key initiative for many organizations, a significant portion are not adequately testing their DR capabilities. Will the desire for simplification and automation increase the adoption of disaster recovery to cloud products and services?

451 Research®
Now a Part of
S&P Global Market Intelligence

Introduction

Though most organizations have deployed disaster recovery infrastructure and or services to provide protection in the event of a disaster, a large portion of organizations are not testing to ensure that these capabilities will actually work when they are needed. In the Voice of the Enterprise: Storage, Budgets and Outlooks 2020 survey, 20% of organizations either were not testing their DR at all or did not have a DR plan to protect their data and infrastructure. With the rapid changes that are being made in production environments, this lack of testing could cause failures to occur when a disaster recovery failover operation is triggered, essentially invalidating the cost and effort expended to deploy them in the first place. Disaster recovery testing continues to be a major challenge for organizations, and it's an area where vendors and service providers are looking to add automation and proactive management capabilities to accelerate and simplify testing to ensure recovery operations and the eventual failback procedure to recover a site will run smoothly when the time arrives.

451 TAKE

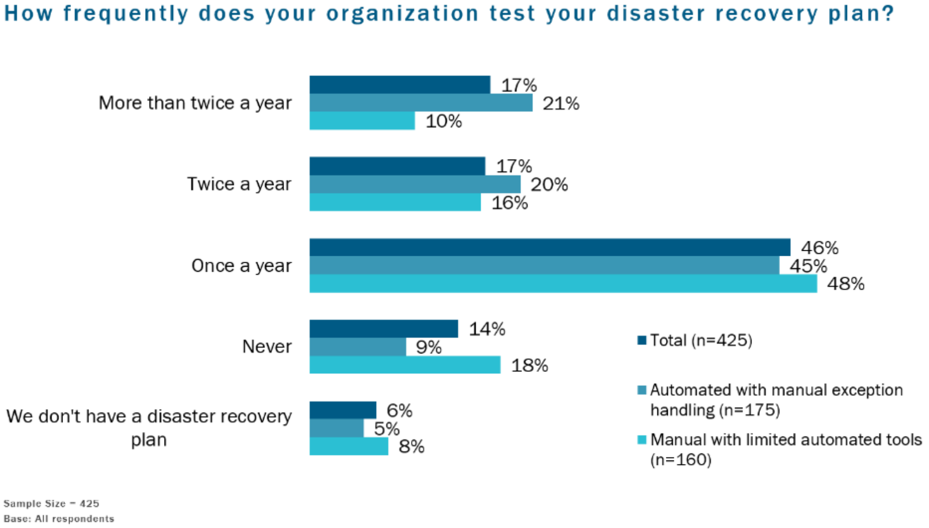
Disaster recovery infrastructure, software and services are the parachute that organizations rely on when everything else around them fails, and right now, most organizations are not making sure these important capabilities will consistently work when needed. This is an issue that will only become worse given that production environments including applications and the underlying infrastructure components are changing and evolving at a rapid pace. This problem represents a major challenge that service providers, infrastructure vendors and data protection software players should be helping their customers overcome. Cloud-based DR has grown in popularity the last few years as companies have looked for lower-cost alternatives to running a conventional DR set up at a remote datacenter or colocation center housing replacement systems.

Most organizations are not testing DR enough

In the Voice of The Enterprise: Storage, Budgets and Outlook 2020 survey, we found that just 17% of organizations surveyed were testing their disaster recovery plans twice a year with an additional 17% testing more frequently than that. On the opposite end of the spectrum, 6% of the respondents admitted their organizations did not even have a disaster recovery plan, while an additional 14% said they never test their DR plans – which is a scary prospect given the importance of uptime and data protection (see figure below).

Most Organizations Are Only Testing Once a Year, or Not at All

Source: 451 Research's Voice of the Enterprise: Storage, Budgets and Outlooks 2020



In the survey, we found that organizations that were mostly automated with manual exception handling were more likely to test twice a year or more (41%) compared to respondents who described their infrastructure management as manual with limited automation tools; only 26% of those respondents said they are testing two or more times per year.

Looking at the responses from various vertical segments, 53% of financial services respondents said they test at least twice a year, which was considerably better than their peers in the healthcare (35%) and manufacturing (20%) segments. In the study, larger companies were testing far more than their smaller counterparts. Nearly half (47%) of companies with over 10,000 employees said they test their DR at least twice a year, in contrast to just 30% of companies under 250 employees with that level of testing.

Perspectives from end users in the field

> *"We haven't really done much testing in the last probably [5-10] years, so that's clearly one of the goals for this year is to try to do at least some testing on the most important stuff [in the DR plan]."*
>
> – Mid-Level Manager, 5,000-9,999 employees, $1-2.49bn, Manufacturing

In our interviews with end users, it was clear that although the subjects understood the importance of having an up-to-date DR plan in place, the maintenance and testing of disaster recovery was not top of mind for many. In the example above, the respondent in the manufacturing sector knew that it had been 5-10 years since the last test and had goals to at least test the DR for their most important workloads in the company's infrastructure.

The lack of DR plan testing reflects a common sentiment that the testing process continues to be extremely time-consuming and manual, which is why this task often gets relegated to the back burner, especially if infrastructure professionals are already struggling to keep up with current business requests and requirements. Ultimately, dropping the ball on current requests and unplanned needs will create a negative business impact immediately, while letting DR testing slide creates a vulnerability that could have an impact in the future. With the increasing customer expectations for rapid resource provisioning and optimization, it is easy to see why IT professionals are prioritizing today's problems.

[“When we test our DR system,] I definitely expect some problems…… The procedures are written but with people who have left the company. The people who are left may not have actually had experience doing it. It may take them a lot longer than [expected]….. [We’ll test] probably just the most important stuff.”

– Mid-Level Manager, 5,000-9,999 employees, $1-2.49bn, Manufacturing

We must remember that DR is not just about technology and automation; it is a human process, and we cannot discount the importance of internal knowledge of business processes and the experience of staffers managing the workloads. As we see in the narrative above (from the same person as the previous narrative), the departure of experienced staff can be a major vulnerability that could trip up a DR plan when it is invoked. It is a key requirement that IT organizations invest time in updating documentation to ensure that teams will be able to run the DR plan efficiently even if the staff that built the plan is no longer at the company or in a different role with no responsibility for maintaining DR. We note that vendors and service providers in the DR space have identified the lack of internal documentation as a key problem, and many have created software and services to help customers create their runbooks and other key assets to fulfill their compliance requirements.

“Just part of [the environment is covered by DR]. The important things to survive because you can’t do everything. It’s impossible. You need to focus on what gets you through the next few weeks if something happened.”

IT/Engineering Manager/Staff, 1,000-1,999 employees, $500-999.9m, Software, IT & Computer

Another key factor is that even in organizations that do have DR in place and are testing consistently, most are focused on projecting a subset of their workloads and not their entire infrastructure, as illustrated in the narrative above. Cost is often brought up as factor for not deploying a comprehensive DR plan to cover all workloads, but as this narrative shows, prioritization of workloads for protection is top of mind for organizations. In many environments, the deployment of DR is limited to mission-critical and business-critical workloads, but even non-critical workloads such as test and dev are getting calls for greater levels of protection and recoverability, and this should intensify as more organizations push to create continuous integration/continuous deployment (CI/CD) environments to accelerate the creation and release of applications.

“[DR tests] happen biannually. They’re reviewed throughout the year, but they have the big test, which shakes the most out…..And through the year, they continually monitor it and say, ‘Hey, what about X?’ and they’ll make tweaks throughout the year, but they don’t make changes to the darn thing daily.”

Mid-Level Manager, 100,000+ employees, $10bn+, Consumer/Retail

The above narrative, which came from a large retail organization, highlights the key reason why the lack of testing is an issue to be concerned with. DR testing for many organizations is a difficult process that is time-consuming and often scheduled to run on a weekend or other relatively idle periods to reduce productivity impact and data loss risks. But we note that even though this particular organization is doing the right thing by testing biannually, even it realizes that because of the constant changes that are made to infrastructure – whether it be the deployment of software patches or the upgrade and replacement of hardware (servers, storage, networking, etc.) – its DR testing has gaps since it cannot account for changes that may have happened between testing cycles.

Recommendations

Integrate DR planning into automation initiatives. Organizations that have invested in automation are able to test their DR plans more consistently, which should make their implementations more reliable in the event of a disaster. The testing process for DR continues to be arduous for most organizations, which explains why so many are not testing enough or at all.

Cloud-based DR has an elastic resource benefit. One of the key benefits of a cloud-based DR implementation in contrast to running DR at a secondary site or a colocation site is the elasticity of cloud. In a cloud-based DR deployment, the bulk of the resource consumption for compute, storage and networking services does not occur until a failover happens. In contrast, traditional environments for DR had matching or similar systems at the failover site, which was a major expense.

Keep staff availability in mind. In the event of a major disaster such as a hurricane or earthquake, it might not be possible for staffers to go to a secondary site to manage the failover process and those resources. Remote management and security will clearly be essential in a DR scenario, but this is also an area where a service provider could be valuable to manage the process and ensure that the replacement resources are running smoothly.

REPORT REPRINT

451 Research®

NEW YORK • BOSTON • SAN FRANCISCO • WASHINGTON DC • LONDON