BLACK & WHITE PAPER

Cloud-Based Disaster Recovery in 2016 and Beyond

DECEMBER 2016

COMMISSIONED BY

About this paper

A Black & White paper is a study based on primary research survey data which assesses the market dynamics of a key enterprise technology segment through the lens of the 'on the ground' experience and opinions of real practitioners – what they are doing, and why they are doing it.

About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
20 West 37th Street
New York, NY 10018
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

LONDON
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 207 426 1050

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

Table of Contents

Executive Summary

Prior to the widespread adoption of virtualization and now the cloud, disaster recovery (DR) was an expensive, complex, labor- and time-consuming proposition. Today, companies can achieve all of the protection afforded by a full-scale plan with cloud-based DR, which provides a considerably less-expensive and more-effective method of attaining total data protection compared to other techniques.

451 Research asked a wide range of organizations about adoption drivers and their use of cloud-based disaster recovery. According to the survey respondents, the top three advantages for adopting cloud DR are faster recovery, improved security and lower operating costs.

Leveraging cloud services for disaster recovery can be beneficial for companies of all types and sizes. For small and midsized businesses (SMBs), turning to the cloud makes fiscal sense. Larger enterprises can use cloud-based disaster recovery to protect their remote, branch and satellite offices, and achieve business continuity – via combined compute, storage and networking services – in the event of primary site failures.

The adoption of cloud-based DR has increased significantly in the last two years. According to our recent end-user survey conducted in October, 64% of organizations have already implemented cloud DR, vs. 46% in Q4 2014. The drivers of this growth are the need to augment or replace an existing system, protect remote and branch offices, and implement disaster recovery if there wasn't a platform already in place. About one-third of respondents indicated that they have a cloud-first strategy/mandate (an approach where cloud is considered or prioritized for all workload deployments) at their company. We see an increasing number of businesses considering cloud as a viable option for disaster recovery and data protection.

The main business benefits organizations expect to gain by relying on the cloud for disaster recovery, as indicated by our survey respondents, include the ability to protect most of their applications and data (not just some of them), as well as to minimize the operational disruption and revenue loss during a downtime or outage.

Another benefit of cloud-based disaster recovery is the ability to more frequently – and remotely – test DR in order to validate the ability to recover after a failure. According to our survey, 74% of organizations that have implemented cloud DR test their plans quarterly or more frequently (compared with 42% in the case of non-cloud-based DR). Cloud-based DR, coupled with a fully virtualized recovery infrastructure, enables more frequent and inexpensive DR testing.

Most organizations we surveyed engage with cloud and IT service providers for cloud DR, and the key quality they look for in a vendor is the ability to provide a cost-effective, reliable and easy-to-use platform that is compatible with their existing IT environment. The option to failover to the cloud to ensure business continuity and resiliency better arms businesses to protect their mission-critical data against any form of operational disruption in a way that is simple, cost-effective and easily managed.

METHODOLOGY

The survey data used in this report was assembled by 451 Research in October 2016 – commissioned by VMware – through a custom survey of 413 IT decision-makers from US- and UK-based midsized businesses (40%) and large organizations (60%) across a wide range of verticals that have deployed or plan to deploy cloud-based disaster recovery. We surveyed organizations that have at least 40% of their primary site (production datacenter) virtualized.

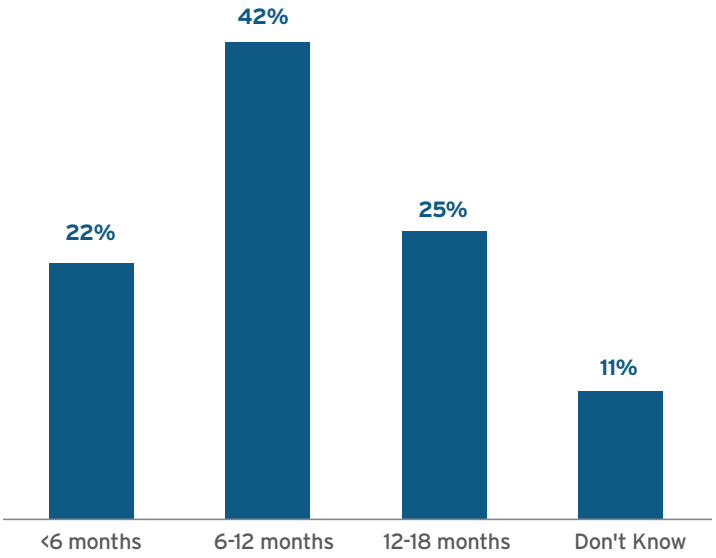
The organizations that participated in our survey pointed to the need to protect, on average, about 350 virtual machines and 15 terabytes of data with their deployments, and we expect to see these numbers rising in the near future.

Overall State of Adoption

The majority of organizations we surveyed (64%) have already implemented cloud-based DR, which is 18% higher than our previous findings two years ago. As shown in Figure 1 below, among companies that don't yet use cloud-based disaster recovery but have plans to do so, 22% will implement it within the next six months and another 42% in 6-12 months. This is similar to the results of the 2014 survey, which shows that the rate of adoption is steady.

Figure 1: Timeline for Implementing Cloud-Based Disaster Recovery

Q: If no solution implemented: What is your expected timeline for implementing a cloud-based disaster-recovery solution?



We asked the participants in our survey about the type of vendor they are using for cloud-based DR and, as shown in Figure 2 below, the preferred vendors are cloud and IT service providers.

Figure 2: Cloud-Based DR Vendor Preference

Q: What type of cloud-based disaster recovery solution vendor do you use today?

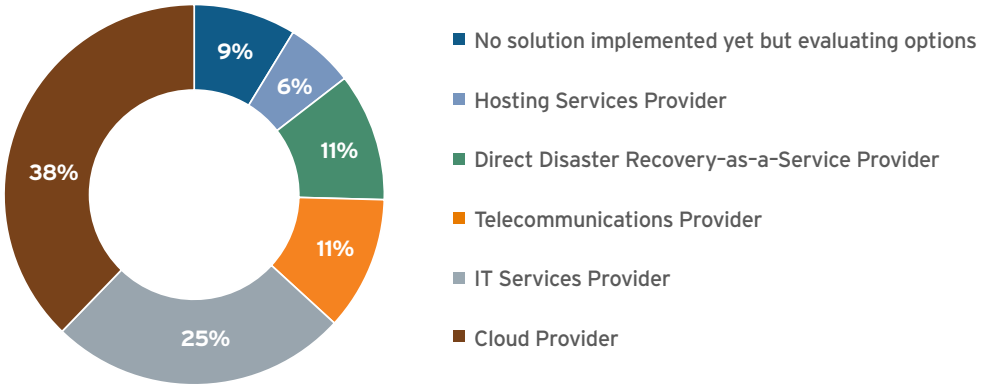
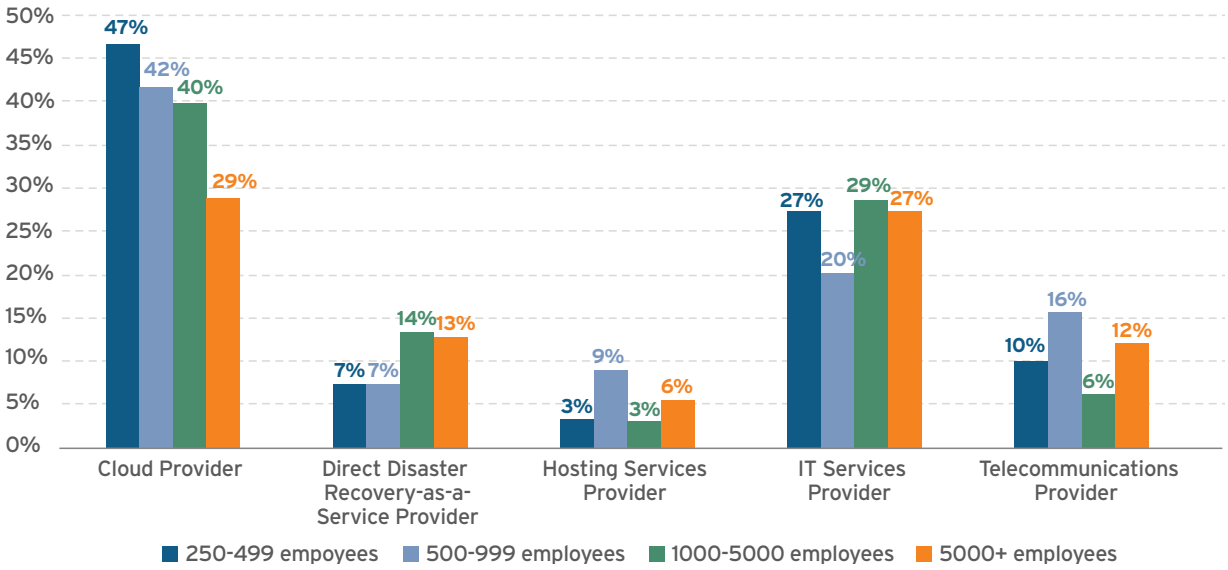


Figure 3: Vendor Preference Based on Size of Company



The type of vendor used by respondents varies somewhat based on the size of the company. For example, while 29% of the largest enterprises in our study use cloud providers for cloud-based DR, that figure jumps to 47% for the smallest organizations (250-499 employees). The use of direct providers jumps from 7% for SMBs (up to 999 employees) to 14% for large enterprises (more than 1,000 employees). Overall, we have seen increased use of cloud providers for 'disaster recovery as a service' implementations, in part due to the variety of service offerings that these vendors provide – they can be a 'one stop shop' for organizations looking for more than one type of cloud service.

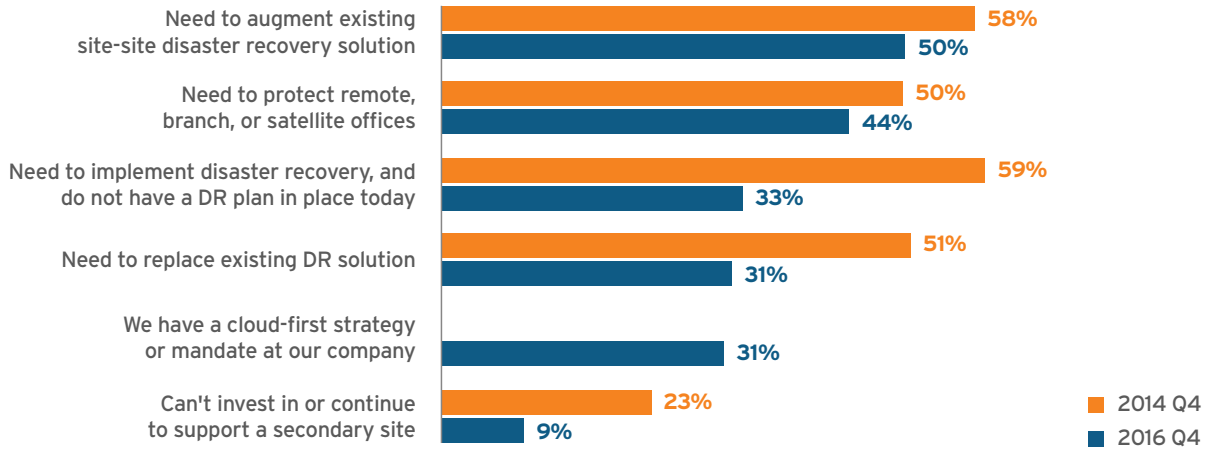
Nevertheless, there is a wide variety of vendors to choose from for cloud-based DR, with different price points and scope of service. It makes sense for end users to work with 'trusted partners' that they already use for their existing infrastructure resources, because having similar technologies at the primary and DR sites also reduces the amount of deployment preparation and testing time that is required.

Business Drivers

What is motivating organizations to adopt, or at least consider adopting, cloud-based disaster recovery? With the growing adoption of cloud DR in the last two years, the key business drivers have somewhat changed. Thirty-three percent of our survey participants do not have a DR plan at all, which is almost half of what respondents reported in 2014 (59%). Today, for most companies, the top two drivers are the need to augment existing technologies and to protect remote, branch and satellite offices.

Figure 4: Cloud-Based DR Primary Business Drivers

Q: What are your primary business drivers for implementing or wanting to implement a cloud-based disaster recovery solution? (select up to three)



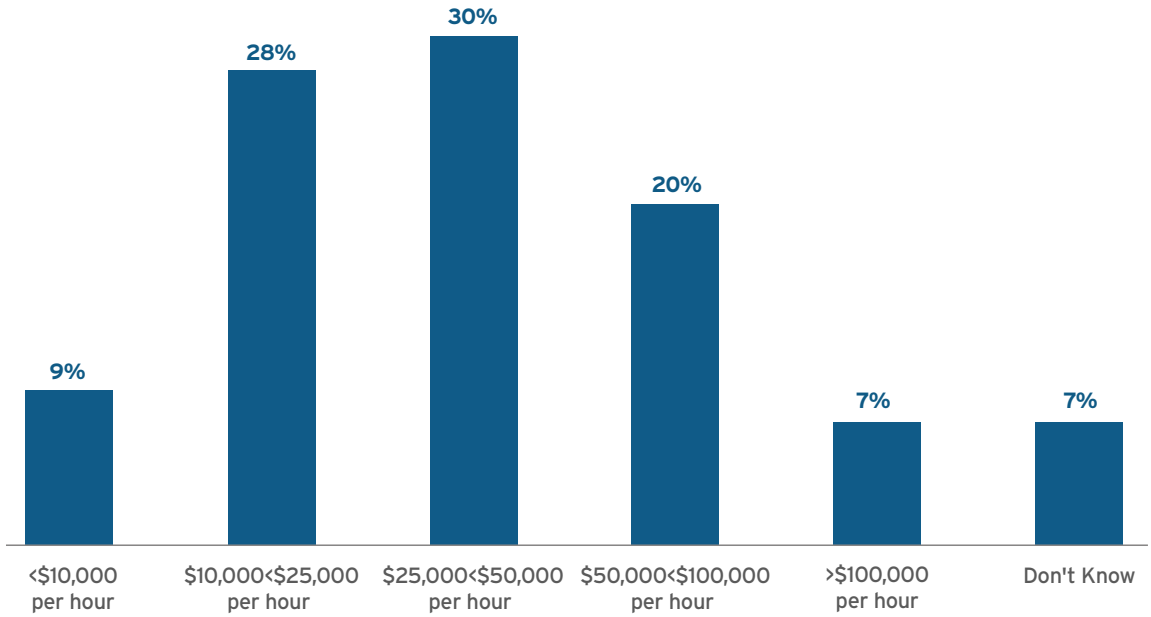
Note: The option "We have a cloud-first strategy or mandate at our company" was not provided in the 2014 survey questionnaire.

About one-third of our survey participants indicated that they have a cloud-first strategy/mandate at their company, which means that IT and lines of business have the responsibility to disqualify cloud as a viable option before considering a non-cloud alternative.

A primary driver behind all disaster-recovery plans is the need to eliminate – or at least significantly decrease – the amount of money lost in the event of site failures or downtime. Even for SMBs, the cost of downtime is staggering: 28% of our survey respondents said that the hourly cost of downtime for their mission-critical applications was $10,000-25,000; 30% put the hourly cost at $25,000-50,000; and 27% estimated that it costs them more than $50,000 per hour (which translates into $1.2m per day).

Figure 5: Estimated Cost of Downtime

Q: What is the estimated cost of downtime per hour for your mission-critical sales applications or production applications?

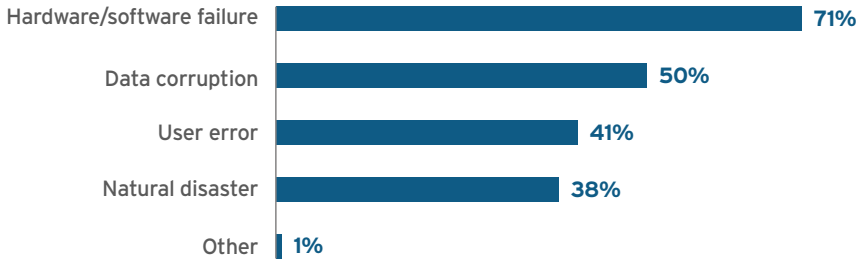


Given the costs of downtime for mission-critical applications, it's easy to see how rapidly companies can realize ROI from a relatively small investment in cloud-based disaster recovery.

But what causes downtime and primary site failures? There is a widespread misperception that the most common causes of primary site failures are natural disasters such as floods, hurricanes, tornadoes and earthquakes. Instead, as shown in Figure 6 below, more common causes of site failures include hardware/software failures (cited by 71% of survey respondents), data corruption (cited by 50%) and user error (indicated by 41% of the participants).

Figure 6: Primary Causes of Site Failure

Q: What has been, or is expected to be, the most common cause for primary site failures? (select up to three)



Requirements

What are the most important requirements for a cloud-based DR platform? The top three requirements highlighted by our survey respondents overall were price (47%), compatibility with existing IT environment (39%) and ease of use (35%). Ease of use is important because IT administrators, rather than storage specialists, are often tasked with DR operations.

The smallest companies (with headcount of 250-499) have a somewhat different set of priorities. For them, the top three requirements are price (40%), flexibility to scale on demand as needed (37%) and ease of use (33%). Flexibility to scale is nearly as important for small businesses as compatibility with existing environment is for larger ones. Cloud can help small businesses operate efficiently as they try to scale.

Figure 7: Key Requirements Based on Company Size

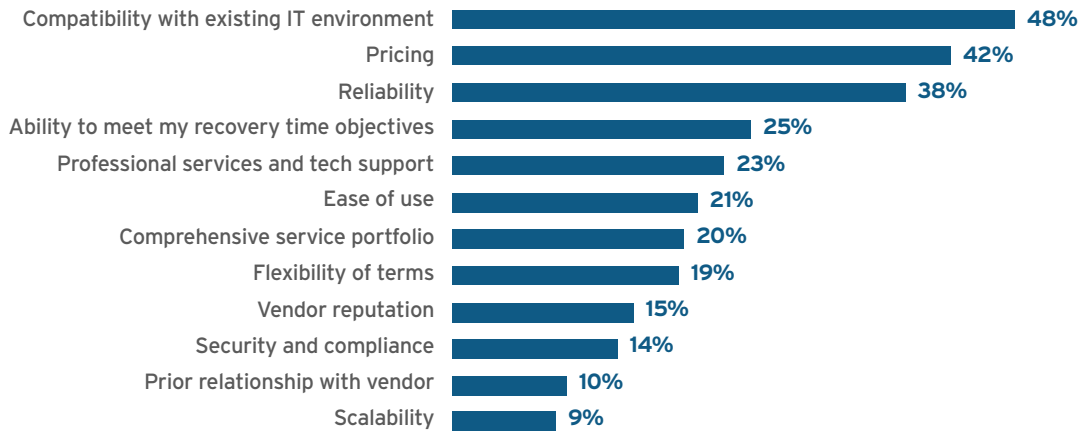
Q: What are the most important requirements for your cloud-based disaster recovery solution? (Select up to three)

	250-499 employees	500-999 employees	1000-5000 employees	5000+ employees	Overall
Price	40%	49%	43%	51%	**47%**
Compatibility with current IT environment	27%	43%	38%	39%	**39%**
Ease of use of the solution	33%	35%	38%	31%	**35%**
Disaster recovery documentation and runbook support	30%	25%	26%	25%	**26%**
Flexibility to scale on demand as needed	37%	25%	23%	26%	**26%**
Self-service ability to customize setting as needed, manage/monitor usage, and perform tasks such as test and declare disaster	17%	24%	30%	25%	**25%**

We also asked our survey participants what they were looking for in a cloud-based DR vendor. Unsurprisingly, compatibility with their existing environments, pricing and reliability were the top three selection criteria, as shown in Figure 8 below. End users are aware that compatibility between primary and DR sites will significantly cut down the time required for deployment and testing. Compatibility with existing IT environment is a higher requirement for larger enterprises.

Figure 8: Key Requirements for Selecting Cloud-Based DR Vendor

Q: What are your key requirements for selecting a cloud-based disaster recovery vendor? (select up to three)

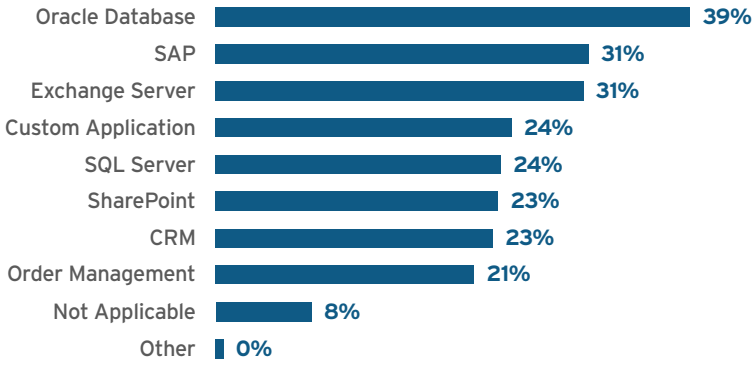


Applications

Oracle Database, SAP and Exchange Server are the top applications that respondents said they protect with DR plans, as shown in Figure 9 below. However, the need to protect Oracle and SAP applications is uncommon among the smallest companies (<500 employees), which have a greater need to protect SQL Server.

Figure 9: Applications Protected with Cloud-Based DR

Q: Have you prioritized workloads to protect? If No, please select 'not applicable'. If yes, which applications and workloads do you plan to protect with a cloud-based disaster recovery solution? (select up to three)



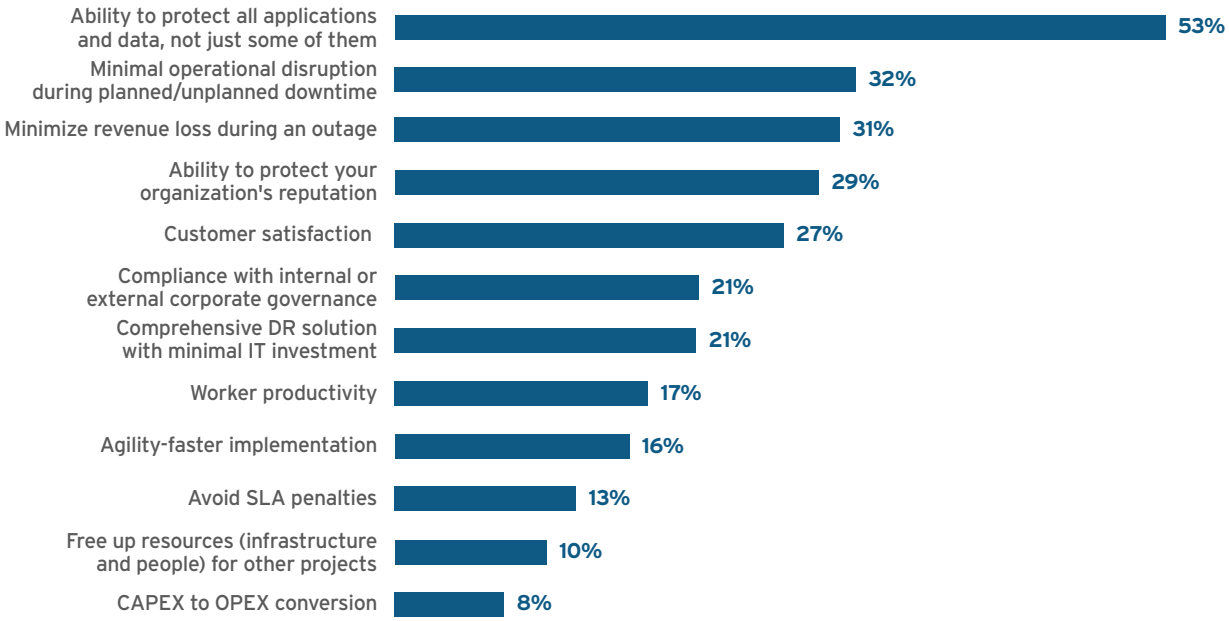
It is critical that organizations first prioritize applications for DR protection and then make sure that prospective providers support all of those applications. And given the relatively low cost of cloud-based DR, companies should consider protecting all of their applications in the cloud.

Business Benefits

In the past, companies had to be selective about which applications to put under DR protection because it was too expensive and complex to protect all of their applications. Cloud has made it both simple and affordable, and consequently, end users consider the ability to protect all of their applications and data to be the primary business benefit of cloud-based DR, as shown in Figure 10 below. Minimizing operational disruption and revenue loss during downtime are other key business benefits that adopters expect from cloud-based disaster recovery.

Figure 10: Expected Business Benefits

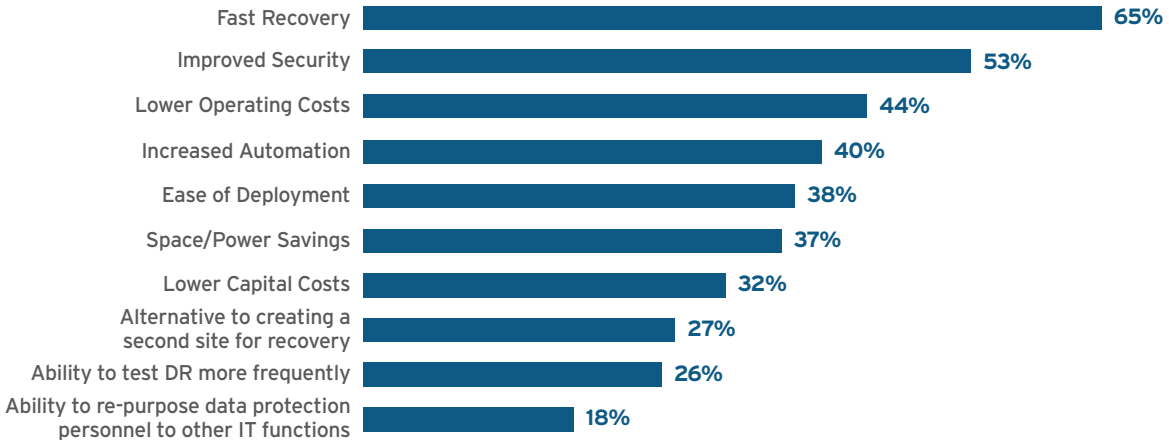
Q: What are your expected business benefits of implementing a cloud-based disaster recovery solution? (select up to three)



In addition to business benefits, organizations value other key advantages of cloud-based DR that differentiate it from other methods of protecting data, such as tape-based vaulting. Given that context, it is not surprising that faster recovery ranked as the number one advantage of cloud-based DR, selected by 65% of the respondents. This was followed by improved security (53%), which is somewhat surprising because the perceived lack of security is often brought up as a primary inhibitor to cloud adoption in general. Other advantages include lower operating and capital costs, increased automation, ease of deployment, space and power savings, increased automation, and the ability to test DR more frequently. Most of these advantages are related to the inherent advantages of cloud computing, including agility, scalability, elasticity and the ability to pay for resources and services on an as-needed basis, which, in the case of DR, means only when a disaster or primary site failure occurs.

Figure 11: Primary Advantages of Cloud-Based DR

Q: What do you believe are the primary advantages of cloud-based disaster recovery? (Select up to five)

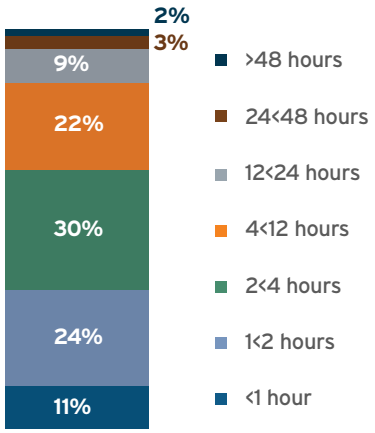


Recovery Times

Recovery times, in the context of DR, are of paramount importance to companies, in large part due to the high costs of downtime during the recovery process. Looking at the total sample in Figure 12 below, only 5% of organizations are willing to tolerate recovery times of more than 24 hours, and 9% said they can tolerate recovery times of 12-24 hours. The majority need much faster recovery times – two to four hours for 30% of our survey participants, and less than two hours for 35% of the companies.

Figure 12: Recovery Time Preference

Q: Recovery times: In the event of a failure at your primary site, how long are you willing to wait until your tier 1 systems/applications are recovered (assuming that the quicker the recovery the more expensive the solution)?



Recovery times provided by cloud-based DR providers are far better than what is typically available via alternative approaches, such as tape vaulting or a secondary site. However, it is important for prospective customers to match their budgets and recovery time objectives (RTO) to the SLAs offered by cloud-based DR providers. These SLAs, which guarantee recovery times, are often offered on a tiered basis with varied pricing levels.

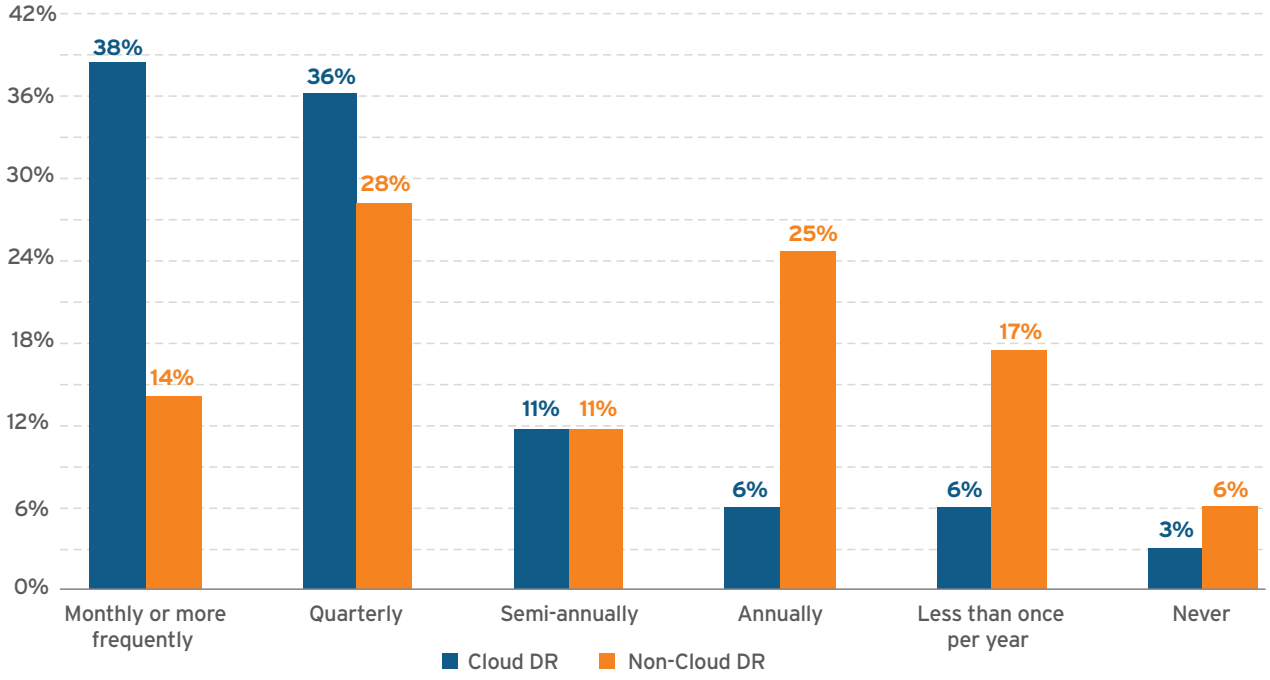
Disaster Recovery Testing

Flexibility to perform failover tests as needed is a key requirement for adopting cloud-based DR, and the ability to do more frequent, automated and affordable DR testing is one of the advantages. After all, if you cannot test your DR capability, how do you know if it will work when needed?

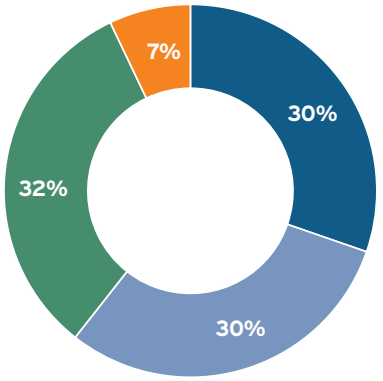
Among companies that have a non-cloud-based DR plan in place, only 14% of them test their DR monthly or more frequently. In contrast, 38% of cloud-based DR users test their DR plan at least once a month, as shown in Figure 13 below. Cloud-based DR makes it much easier and less expensive to run DR tests.

Figure 13: Cloud-Based vs. Non-Cloud Based DR Plan Testing

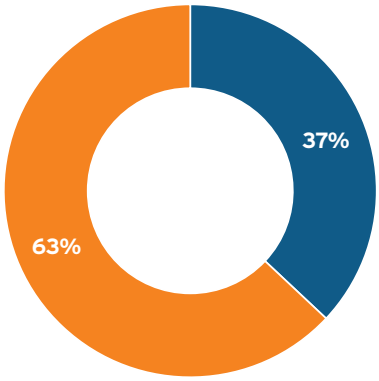
Q: How often do you test your plan?



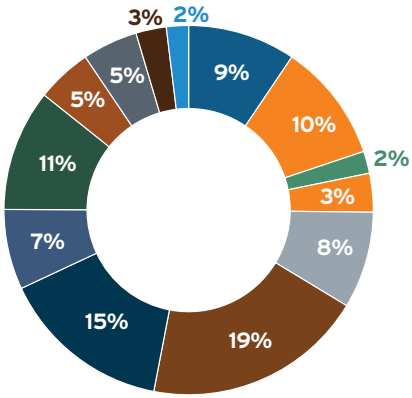
Appendix: Survey Demographics



- More Than 5000 employees
- 1000-5000 employees
- 500-999 employees
- 250-499 employees

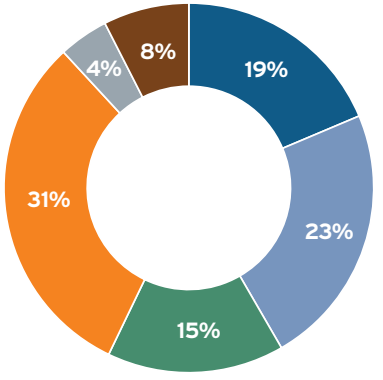


- United Kingdon
- United States

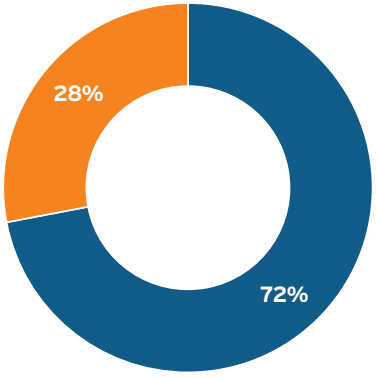


- Other
- Retail
- Services
- Telecommunications
- Transportation
- Utilities
- Education
- Finance
- Government-Local
- Government-State/National
- Healthcare
- Information Technology
- Manufacturing

Respondents

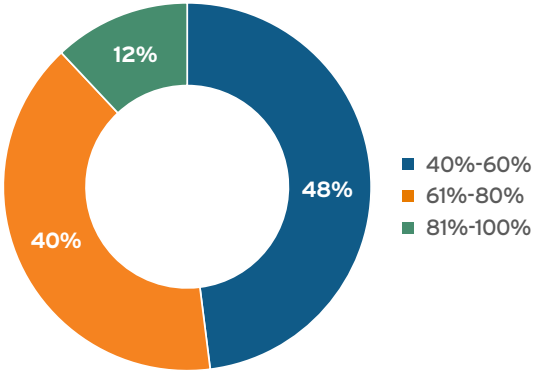


- C-Level
- Director
- IT administrator
- Manager
- Other
- VP



- I am a decision-maker for IT
- I am involved/influence the decision-making for IT

Level of Virtualization of Primary Site



Current Use of Cloud DR