451 Research | Advisory Services

Drivers for the Growing Adoption of Cloud-Based Disaster Recovery

PREPARED FOR VMWARE BY 451 RESEARCH

JAN 2015

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.

The information contained herein has been obtained from sources believed to be reliable. 451 Research disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although 451 Research may discuss legal issues related to the information technology business, 451 Research does not provide legal advice or services and their research should not be construed or used as such. 451 Research shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

451 Research®

New York
20 West 37th Street, 6th Floor
New York, NY 10018
Phone: 212.505.3030
Fax: 212.505.2630

San Francisco
140 Geary Street, 9th Floor
San Francisco, CA 94108
Phone: 415.989.1555
Fax: 415.989.1558

London
Paxton House (5th floor), 30 Artillery Lane
London, E1 7LS, UK
Phone: +44 (0) 207 426 0219
Fax: +44 (0) 207 426 4698

Boston
125 Broad Street, 4th Floor
Boston, MA 02109
Phone: 617.275.8818
Fax: 617.261.0688

TABLE OF CONTENTS

INTRODUCTION AND METHODOLOGY

VMware has commissioned 451 Research to produce an independent report on the adoption of cloud-based disaster recovery (DR). This report is intended to provide an objective assessment of the business drivers, requirements and expected benefits of cloud-based DR, as well as to highlight the main trends that characterize the current state of adoption. The intended audience for this report includes IT decision-makers from small and medium-sized businesses (SMBs) through to larger enterprises that are considering implementing a cloud-based DR solution.

KEY FINDINGS

Utilizing the cloud yields a wide variety of benefits, and one of the most obvious and straightforward cloud use cases is disaster recovery in support of business continuity for an organization. In fact, 451 Research believes that DR is the low-hanging fruit in terms of end-user cloud adoption – in other words, the advantages are so obvious and the ROI so rapid that DR is an excellent way to get started with using cloud-based service delivery. 451 Research user survey data has shown that backup and disaster recovery are consistently among the top three compelling reasons for companies to consume Infrastructure as a Service (IaaS). In addition to spurring adoption of cloud computing overall, cloud-based DR provides a considerably less expensive and more effective method of attaining total data protection compared with existing techniques.

We think the business case for enterprises to cut over to the cloud for their DR operations differs from that of SMBs. For SMBs, turning to the cloud makes good fiscal sense, and in fact many SMBs are evaluating – and some have already implemented – cloud-delivered DR. Based on the research presented in this report, many more will do so over the next 12 to 18 months. For enterprise organizations, cloud-based DR is also very attractive, especially for their remote offices and branch offices (ROBOs), to protect their IT assets and achieve business continuity in the event of primary site failures or disasters.

Prior to widespread adoption of virtualization and the viability of the cloud for IT operations, disaster recovery was an extremely expensive, complex, and labor- and time-consuming proposition. The 'old school' methodology of implementing DR – affordable only to the largest of IT organizations – involved building or leasing a secondary site for DR purposes. Further compounding the high cost factor, IT organizations essentially had to buy the same – very expensive – hardware at the DR site that they deployed at the central production site. In addition, this approach involved costly replication and redundant software licenses for the secondary site. This mode of DR was simply too expensive and complex for many organizations, particularly SMBs. But with virtualization, and later the cloud, many more companies can now achieve all of the protection afforded by a full-scale DR setup.

As the 451 Research survey results presented in this report will show, early adopters have achieved a number of benefits from relying on the cloud for their DR implementations. The most obvious benefit is cost savings. In most cases, the cost savings are extreme because businesses do not have to invest in (or lease) their own physical datacenter and IT infrastructure for DR purposes. As such, they can virtually eliminate the capital expenditure (capex) typically associated with DR infrastructure. Just as important are the cost savings in operating expenditure (opex), much of which is assumed by the cloud provider, which significantly decreases the amount of personnel and time typically associated with maintaining DR operations.

Another benefit of cloud-based DR is the ability to more frequently – and remotely – test DR function in order to validate the ability to recover after a failure at the primary site. After all, how do you know if your recovery will work when needed if you don't test it frequently? According to 451 Research studies, even IT organizations that have implemented expensive DR facilities do not test them more than once per year (or, often, even less frequently). Cloud-based DR, coupled with a fully virtualized recovery infrastructure, enables more frequent and inexpensive DR testing.

A further advantage with cloud-based DR cited frequently by our survey participants is the ability to significantly decrease their all-important recovery time objectives (RTO) and recovery point objectives (RPO). In fact, some cloud-based DR service providers can recover infrastructure within four hours – compared with recovery times that were measured in days with 'old school' methods such as recovering from off-site tape vaults. Today, cloud-based DR vendors can provide an RPO of as little as 15 minutes, which can sometimes be set on a per-VM level of granularity.

In addition to providing the ability to *failback* to the primary site after recovering from whatever the original disruption entailed, cloud-based DR more importantly provides an inexpensive way to *failover* to the cloud in the event of a failure, thus providing business continuity via combined compute, storage and networking services. This is accomplished by simply spinning up VMs and related data in the cloud. And some cloud-based DR service providers offer 'hot, warm and cold' failover alternatives, depending on customers' budgets and RTO/RPO requirements.

The option to now failover to the cloud in order to ensure business continuity and resiliency better arms companies to protect their mission-critical data against any form of operational disruption in a way that is simple, affordable and easily managed. In addition, failover to the cloud enables companies to avoid lost revenue and/or employee productivity due to downtime.

METHODOLOGY

The data used in writing this report was compiled through a custom survey of 403 IT decision-makers from US-based small and medium-sized businesses, as well as some larger enterprises that have deployed – or plan to deploy – a cloud-based disaster-recovery solution. In addition, we incorporated further insight from other proprietary data sets owned by 451 Research, as well as leveraging the subject-area knowledge and expertise of our analysts.

CLOUD DISASTER RECOVERY

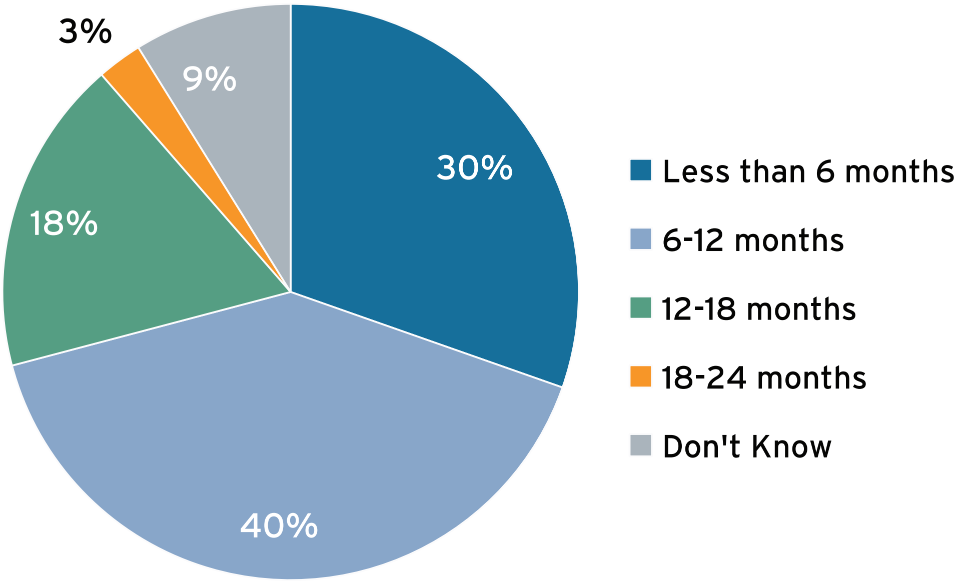
State of Adoption

According to 451 Research Market Monitor data, the cloud-based backup and recovery market is expected to grow at a 21% CAGR over the next several years, with almost all of the adoption occurring in the SMB segment of the market. Some SMBs have already implemented cloud-based disaster recovery, but even more encouraging is how quickly the rest of the market plans to embrace the cloud for their DR requirements.

As illustrated in Figure 1, among companies that have not yet implemented cloud-based DR but have plans to do so, 30% will implement it within the next six months, and another 40% plan to implement it in 6-12 months. Considering the fact that many organizations were not even aware of the cloud-based option for DR a few years ago, this is an astounding rate of adoption.

FIGURE 1: TIMETABLE FOR IMPLEMENTING CLOUD-BASED DR

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

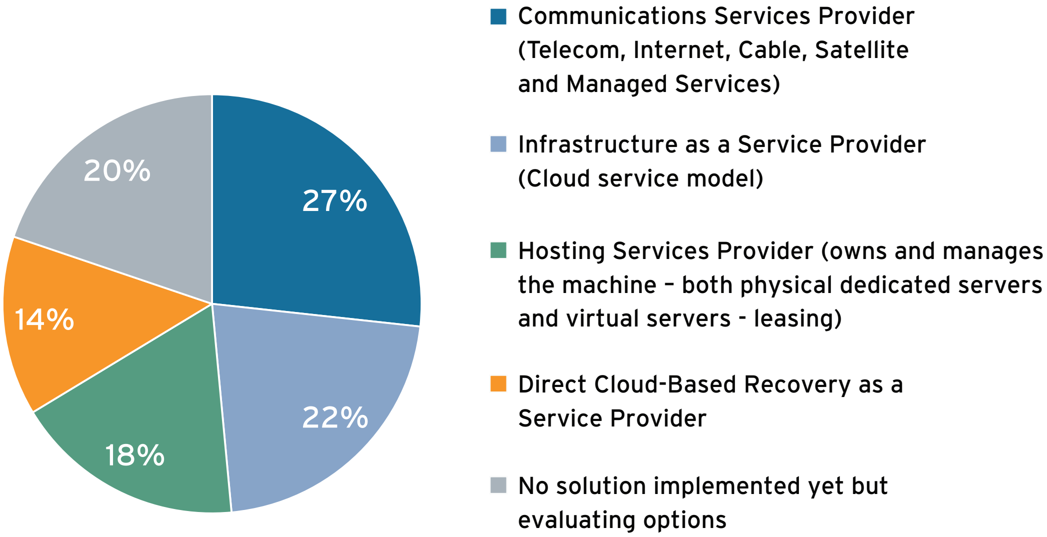


n=79

There are currently a wide variety of options in terms of the types of vendors that offer cloud-based DR, which can sometimes lead to confusion among prospective customers. It could also lead to consolidation in the market, which is another reason why it is critical for companies to be very diligent in choosing a vendor. We asked the participants in our survey what type of vendor they are using for cloud-based DR and, as illustrated in Figure 2, there is a fairly even split among the various vendor options.

FIGURE 2: CLOUD-BASED DR VENDOR PREFERENCE

Q. What type of cloud-based disaster-recovery solution vendor do you use today? [Select one]



n=403

The type of cloud-based DR vendor used by respondents varies somewhat based on the size of the organization. For example, while 21% of the smaller SMBs (less than 500 employees) in our study use communications service providers for cloud-based DR, that figure jumps to 35% among the larger midsized companies (1,000-5,000 employees). Similarly, the use of IaaS providers jumps from 14% for smaller SMBs to 25% for midsized companies. Recently we have seen increased use of IaaS vendors for DR-as-a-service (DRaaS) implementations, in part due to the variety of service offerings that IaaS vendors provide. This effectively provides a 'one-stop shop' for organizations looking for more than one type of cloud service.

The salient point here is that there is a wide variety of vendor options for cloud-based DR, with different price points and scopes of service. Our advice is to give evaluation preference to 'trusted partners' that you already deal with for existing infrastructure resources, including software and hypervisor platforms and management tools. Having similar technologies – particularly virtualization technology – in the primary and DR environments also reduces the amount of deployment preparation and testing time that will be required.

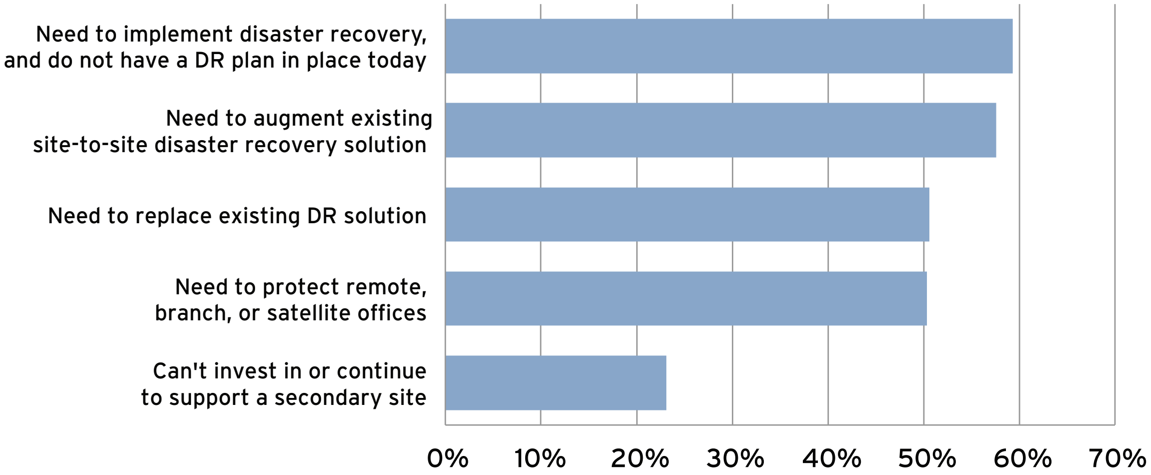
KEY DRIVERS AND REQUIREMENTS

BUSINESS DRIVERS

What is motivating organizations to adopt, or at least consider adopting, cloud-based disaster recovery? As illustrated in Figure 3, there are a number of primary drivers, with a fairly even distribution among our survey participants.

FIGURE 3: 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]



n=403

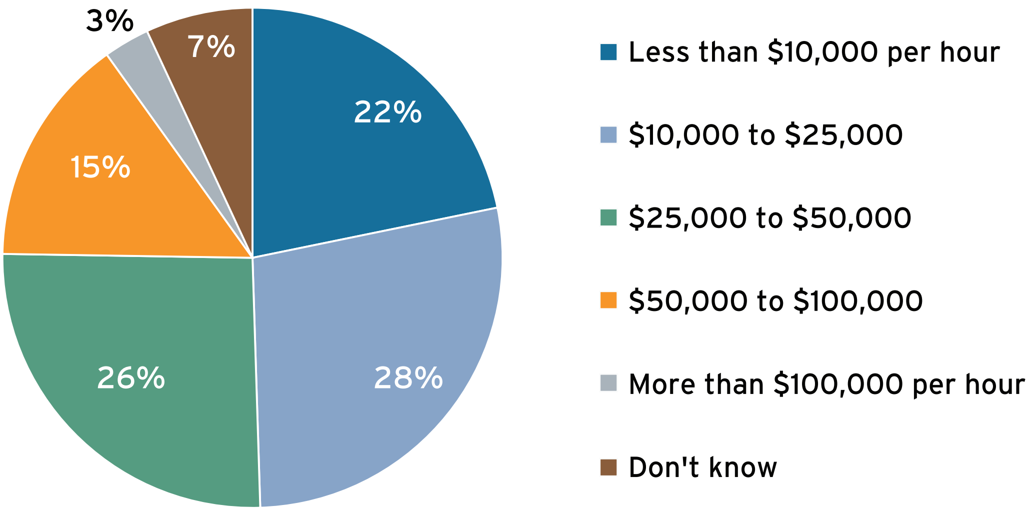
Most companies today are aware that they need to have a disaster-recovery plan but, due primarily to the high costs previously associated with implementing DR (prior to wide-spread adoption of virtualization and the cloud), they simply haven't been able to afford it. As illustrated in Figure 3, almost 60% of our survey participants do not have any DR plan at all. In these cases, end users are motivated by the relatively low cost of cloud-based DR.

About half of our survey participants cited the need to replace their existing DR solutions. Another popular business driver behind adoption of cloud-based DR is the requirement to protect remote offices and branch offices without the costly option of centralizing backup/recovery at the primary production site. And although many businesses do not even have a secondary site for DR purposes, 22% of survey respondents said they can no longer afford to build, lease and/or support a secondary site, as illustrated in Figure 3.

Of course, 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, whether planned or unplanned. Even for SMBs, the cost of downtime is often staggering. For example, 28% of our survey respondents said that the hourly cost of downtime (including lost revenue, as well as lost productivity and operational costs) was between $10,000 and $25,000; 26% put the hourly cost at $25,000-50,000; and 18% estimate that it costs them more than $50,000 per hour – which translates into $1.2 million per day.

FIGURE 4: ESTIMATED COST OF DOWNTIME

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

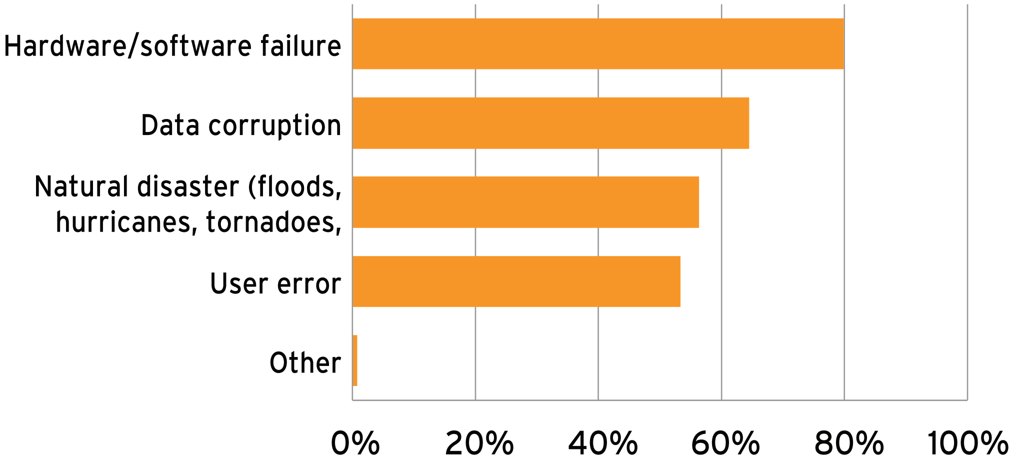


Given the huge cost of downtime for mission-critical applications, it's easy to see how rapidly companies can realize ROI from a relatively small investment in cloud-based disaster recovery.

What causes downtime and primary site failures? It's a widespread misperception that the most common causes of primary site failures are natural disasters such as floods, hurricanes, tornadoes and earthquakes. Instead, as illustrated in Figure 5, more common causes of site failures include hardware/software failures (cited by 80% of survey respondents) and data corruption (cited by 65% of respondents). And simple user error accounts for about as many site failures as do natural disasters.

FIGURE 5: CAUSES OF PRIMARY SITE FAILURES

Q. What has been, or is expected to be, the most common cause for primary site failures? [Select up to three]



n=403

REQUIREMENTS

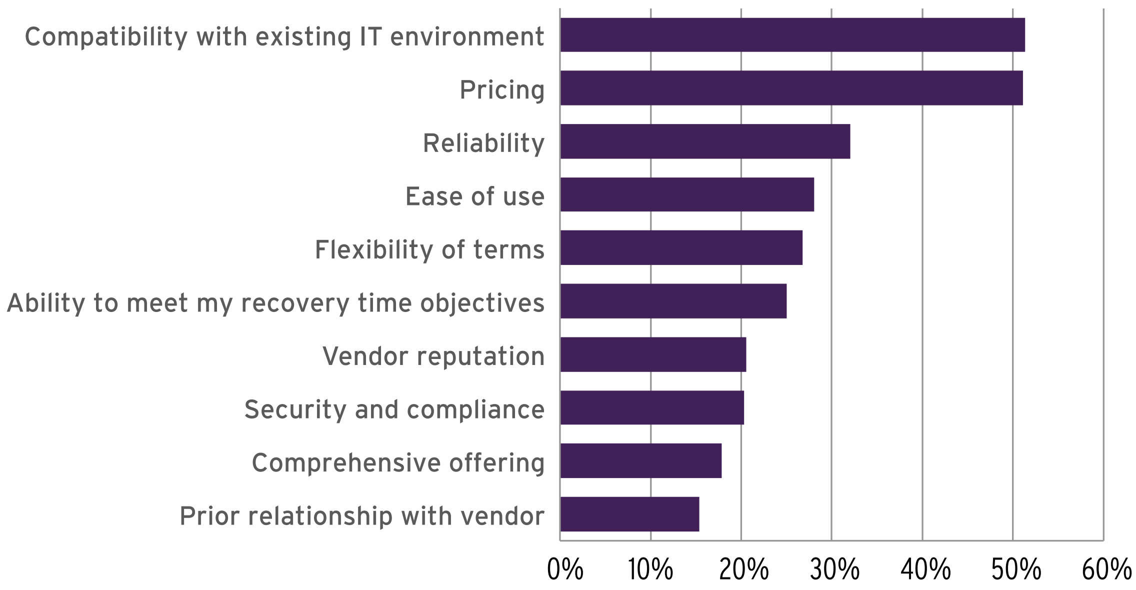
We queried our survey participants about their most important requirements in a cloud-based DR solution. The top two requirements – each cited by more than 50% of respondents regardless of company size – were price (59%) and ease of use (52%). Ease of use is particularly important because it is often VM administrators, rather than storage specialists, that are tasked with DR operations. These responses were not surprising given the state of IT budgets today, as well as the density of input from SMB respondents in this survey.

However, other top requirements, in decreasing order, include compatibility with users' existing environment; self-service (the ability for end users, rather than just the providers, to customize settings, manage/monitor usage, and perform DR testing); flexibility to scale on demand as needed; automation/orchestration of failover/failback; the ability to set and meet recovery time objectives; and the ability to do failover tests as needed.

We also asked survey participants what they were looking for in a cloud-based DR vendor. Again, not surprisingly, pricing and compatibility with their existing environments were the top selection criteria – cited by more than half of respondents – as illustrated in Figure 6. End users are aware that compatibility between the primary and DR environments will significantly cut down on the time required for deployment and testing.

FIGURE 6: 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]



n=403

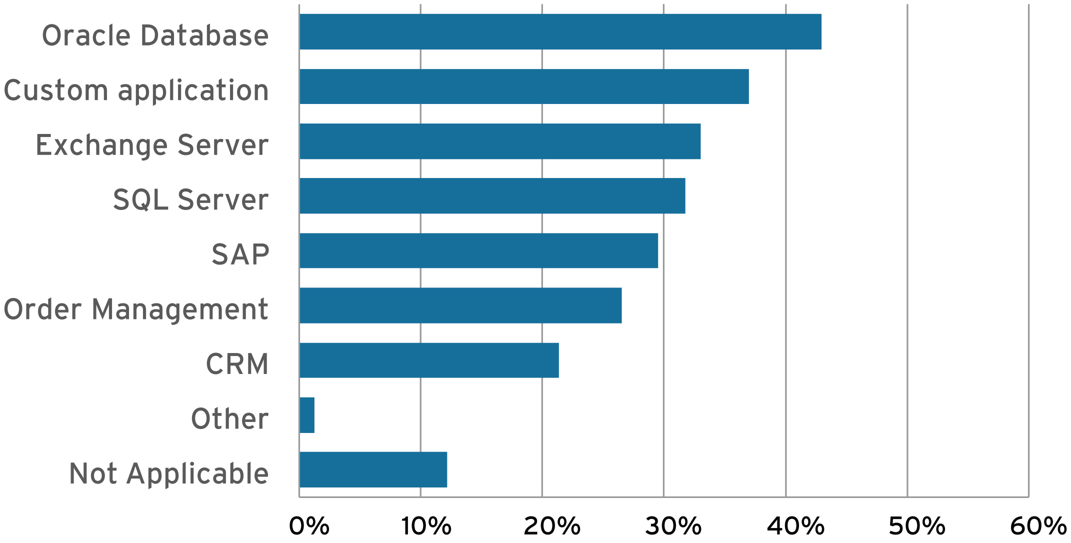
Although there weren't many surprises among the responses to this question, we would call attention to the importance of both vendor reputation and a prior relationship with the vendor. The cloud-based DR market will in all likelihood be crowded with a number of small vendors that may or may not survive, and it is critical that a customer has a comfort level with their supplier based on an existing relationship and proven technology.

PRIMARY WORKLOADS

Since our survey included a fair amount of SMBs, we were not surprised to see that users ranked Windows applications such as Exchange Server and SQL Server among the applications they would prioritize for DR protection. But we were somewhat surprised that Oracle databases and custom applications were the top two application choices that respondents said they need to protect with DR plans, as illustrated in Figure 7.

FIGURE 7: WORKLOADS 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]



n=403

Although Oracle and custom applications are not as common as Windows applications in SMB environments, they are deemed more mission-critical by some organizations. The need to protect Oracle and custom applications – as well as SAP and CRM environments – was considerably higher among SMBs with relatively large IT budgets (over $10m).

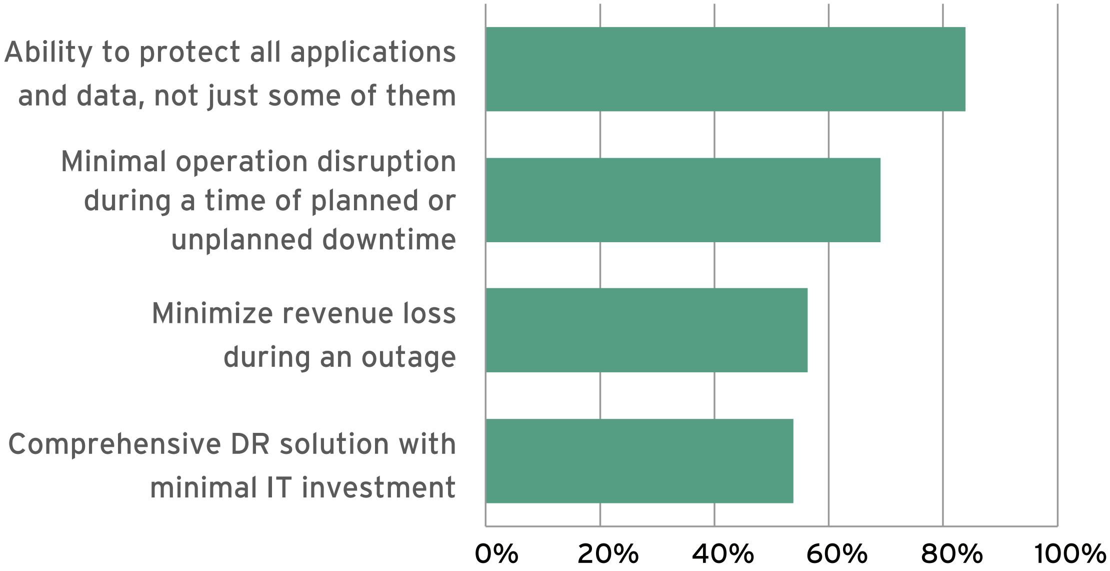
It is critical that organizations first prioritize applications for DR protection and then make sure that prospective providers support all of those applications. And, given the relatively low cost of cloud-based DR, we would encourage companies to consider protecting all of their applications in the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

BUSINESS BENEFITS AND ADVANTAGES

In the past, companies had to be selective about what applications to put under DR protection because it was simply too expensive, time-consuming and complex to protect all of their applications. As such, they tended to protect only the most mission-critical applications and data, and leave other applications unprotected by DR plans. But now that the combination of virtualization and the cloud has made DR both simple and affordable, end users consider the ability to protect all of their applications and data to be the primary business benefit of cloud-based DR, as illustrated in Figure 8.

FIGURE 8: EXPECTED BUSINESS BENEFITS

Q. What are your expected business benefits of implementing a cloud-based disaster-recovery solution? [Select up to three]



n=403

As discussed previously, minimizing both revenue loss and operational disruption during downtime – either planned or unplanned – are other key benefits that adopters expect from cloud-based disaster recovery. And the relative ranking of business benefits was about the same across companies of all sizes in our study.

In addition to querying organizations on their expected business benefits, we asked them what the primary advantages of cloud-based DR were relative to other methods of protecting data, which, in many cases, consisted of tape-based vaulting. Given that context, it is not surprising that faster recovery ranked as the number one advantage of cloud-based DR, cited by 69% of respondents. This was followed closely by improved security (61%), which was somewhat surprising because a perceived lack of security is often cited as a primary barrier to cloud adoption in general. But the fact that our survey participants ranked improved security as the second-biggest advantage of cloud-based DR tells us that security is no longer as much of a burning concern when it comes to cloud adoption.

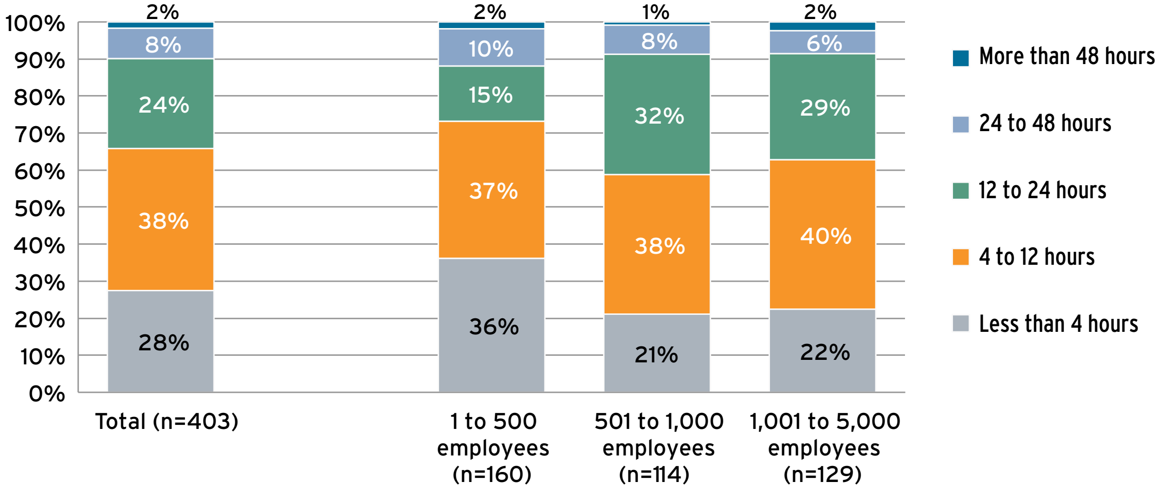
In decreasing order, the other primary advantages of cloud-based DR included ease of deployment, lower operating and capital costs, space and power savings, increased automation, the ability to test DR more frequently, and the ability to repurpose data-protection personnel. Although a lot of these advantages are directly related to the benefits of using virtualized resources in the DR infrastructure, all of them are related to the inherent advantages of cloud computing, including agility, scalability, elasticity, and the ability to pay for resources and services only on an as-needed basis – which, in the case of DR, means only when a disaster or primary site failure occurs. As another cost savings, cloud-based DR eliminates the need for additional capex.

RECOVERY TIMES

In the context of DR, recovery times are of paramount importance to most companies, in large part due to the high costs of downtime during the recovery process (as covered in a previous section of this report). Looking at the total sample in Figure 9, only 10% of our survey respondents can tolerate recovery times of more than 24 hours, and 24% can tolerate recovery times of 12-24 hours. The majority, however, need much faster recovery times – 4-12 hours for 38% of survey participants, and less than 4 hours for 28% of them. Looking at the breakdown across the three company-size segments, there was little difference between their recovery time objectives.

FIGURE 9: RECOVERY TIME PREFERENCES

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)?



Fortunately for end users, most cloud-based DRaaS providers can meet the most stringent recovery time objectives. However, it is important for prospective customers to match their budget and RTOs to the service-level agreements offered by cloud-based DR providers. These SLAs, which guarantee recovery times, are typically offered on a tiered basis, with varying price levels.

The recovery times provided by cloud-based DR providers are far better than what is typically available via alternative approaches to DR, such as tape vaulting or a secondary site. For example, 42% of survey respondents that had previously used tape-based DR reported recovery times in excess of 12 hours, and 19% experienced recovery times of more than one day. Bearing in mind the cost of downtime reported by survey participants, it is easy to see how shaving off even a few hours of recovery time can translate into major cost savings.

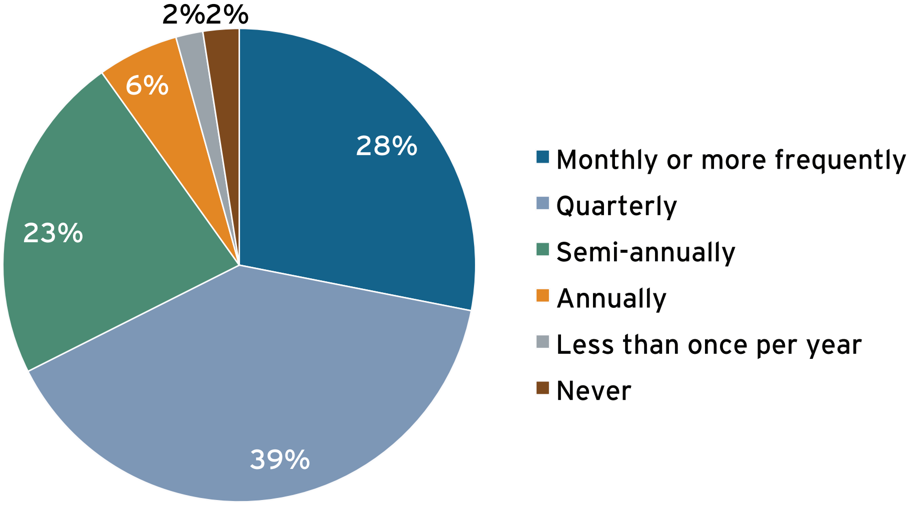
THE NEED FOR DR TESTING

As we've mentioned, the flexibility to perform failover tests as needed is one of the key requirements in adopting cloud-based DR. And the ability to do more frequent, automated and affordable DR testing is one of the big advantages of cloud-based DR. After all, if you cannot test your DR capability, how can you know if it will work when needed?

Among companies that have a DR plan in place that is not cloud-based, only 11% of them test their DR monthly or more frequently. By contrast, 28% of cloud-based DR users test their plan at least once a month, as illustrated in Figure 10.

FIGURE 10: CLOUD-BASED DR PLAN TESTING

Q. If you have already implemented a cloud-based disaster-recovery solution, how often do you test your plan?



n=324

What's truly startling is the fact that 33% of non-cloud DR users *never* test their DR plan. Among cloud-based DR users, that figure drops to only 2%, as illustrated in Figure 10. Cloud-based DR makes it much easier and much less expensive to run DR tests.

RECOMMENDATIONS FOR USERS

451 Research recommends that companies first perform a cost analysis of the various options for disaster recovery (traditional second-site DR, tape-based vaulting, cloud-based DR). They should then develop a DR plan, or blueprint. This begins with prioritizing applications to protect under the DR plan (preferably, all applications).

Next, determine how much downtime is acceptable for each application, or group of applications, in order to determine the right RTO and RPO.

In evaluating potential vendors, give priority to 'trusted partners' with whom you have prior experience. Also be sure to choose a vendor that bases its cloud DR infrastructure on proven technologies and providers. Disaster recovery is not a use case where taking chances is an option.

Organizations should then determine whether the cloud-based DR vendor offers SLAs that match the company's RTO and RPO requirements – as well as their budgetary requirements.

Cloud-based disaster recovery, or DRaaS, is an emerging option for businesses of all sizes to attain affordable, simple protection of applications and data from losses associated with disasters or primary site failures. Today, many of the initial barriers to adoption have been addressed, and based on our market research data, we expect a surge in adoption of cloud-based DR over the next couple of years.

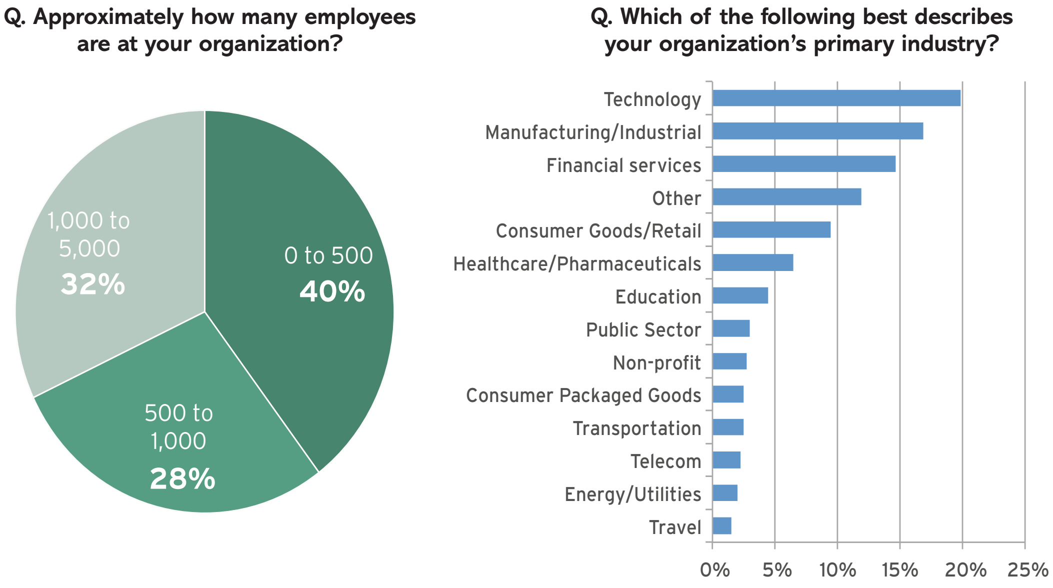
APPENDIX

SURVEY DEMOGRAPHICS

451 Research surveyed 403 US-based small and medium-sized businesses (40% - less than 500 employees), as well as larger enterprises (60% - 500 to 5,000 employees), that have deployed or are planning to deploy a cloud-based disaster-recovery solution. About half (46%) of the survey respondents have already implemented cloud-based DR, while the remaining 54% plan to implement cloud-based DR in the near future.

Our survey demographic was split fairly evenly by company size and vertical industry, as illustrated in Figure 11.

FIGURE 11: RESPONDENTS BY COMPANY SIZE & INDUSTRY


Q. Approximately how many employees are at your organization?

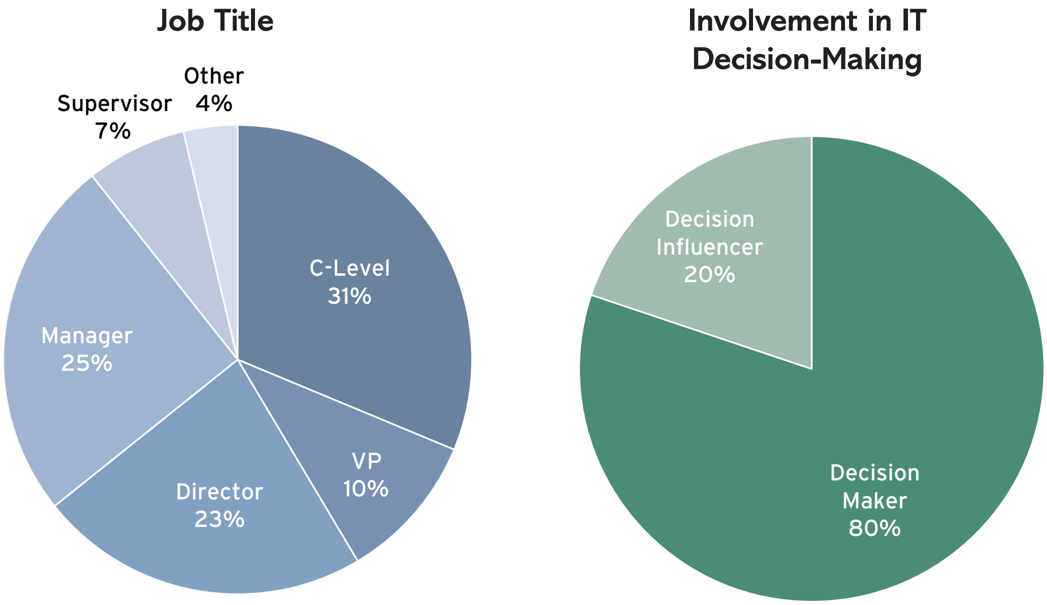
Q. Which of the following best describes your organization's primary industry?

n=403

Of those participating companies, 14% have an IT budget of less than $100,000, while 56% range from $100,000 to $5m, and 29% have IT budgets in excess of $5m.

We focused on managerial-level professionals, and only included users that were either IT decision-makers or those who influence technology and services procurement, as illustrated in Figure 12.

FIGURE 12: RESPONDENTS BY JOB AND DECISION-MAKING RESPONSIBILITY



Job Title

Involvement in IT Decision-Making