Enterprise Strategy Group | **Getting to the bigger truth.™**

ESG Research
Final Sponsor Report

The Evolving Business Continuity and Disaster Recovery Landscape

By Jason Buffington, Senior Analyst

With Bill Lundell, Senior Research Analyst & Jennifer Gahm, Senior Project Manager

January 2016

Contents

List of Figures

Executive Summary

Report Conclusions

ESG surveyed 391 North American IT professionals representing midmarket (100 to 999 employees) and enterprise-class (1,000 employees or more) organizations in order to explore the trends and preferences involving business continuity and disaster recovery (BC/DR) strategies, implementations, and methodologies. All respondents were IT professionals familiar with and/or responsible for data protection technology decisions for their organization, specifically around technologies and processes to facilitate BC/DR.

Based on the data collected from this survey, ESG concludes that:

- **Today's approaches to recovery are insufficient for the IT resiliency requirements**, with downtime tolerances and intended SLAs being higher than current recoverability methods or traditional means of protection and restoration can achieve.
- **Cloud-based services are a growing part of many BC/DR strategies**, including not only the use of disaster recovery-as-a-service (DRaaS) offerings, but also infrastructure-as-a-service (IaaS) for hybrid architectures, as well as simply utilizing natively resilient software-as-a-service (SaaS) platforms for their continuity and data survivability purposes.
- **Both DR services and self-managed BC/DR facilities are growing in usage**, in part due to the reduced complexity of newer availability/BC technologies, as well as a heightened understanding of the modern SLAs and intolerance to downtime faced by organizations of all sizes.
- **BC/DR is recognized as much more than "backup,"** with backup administrators in the minority of BC/DR planning and execution teams. Instead, most BC/DR strategies are planned and enacted by IT operations teams and VP-IT/CIO leadership functions, with backup administrators taking a supporting role in much the same way that other platform or workload owners might.

Introduction

Research Objectives

ESG routinely sees *business continuity and disaster recovery* as one of the top ten IT priorities in its annual IT spending intentions research (including 2015's iteration).[1]

In order to gain insight into what IT professionals and their leadership are doing around BC/DR preparedness, the survey was designed to answer the following questions:

- What is the amount of downtime organizations can tolerate from their primary production servers or systems before making the decision to "fail over" to a BC/DR secondary site or service provider for "high priority" applications compared to "normal" production workloads?
- What methods are being used to facilitate disaster recovery strategies?
- What methods are used to replicate data between sites for the purposes of BC/DR or IT resiliency?
- Approximately what percentage of production servers can currently resume functionality at a secondary BC/DR site or service of some kind? How will this change over the next 24 months?
- How often do organizations execute test recoveries to determine if/how quickly they can recover from their BC/DR site or service provider systems in the event of an outage?
- On average, approximately what percentage of routine tests for BC/DR preparedness succeed or "pass"?
- What types of BC/DR events have caused organizations to leverage a secondary site or infrastructure as part of their IT recovery experience?
- How many times in the past year have organizations had to "fail over" to or resume functionality of even a single production server/VM from existing BC/DR secondary sites?
- How many times in the past year have organizations had to "fail over" to or resume functionality of an entire server room or site from existing BC/DR secondary sites?
- What would cause organizations to change or add a new BC/DR site or service provider(s)?
- What roles or groups are actively involved in planning and scoping out BC/DR strategies? Which group is ultimately charged with enacting the BC/DR strategy?
- How frequently are BC/DR strategies assessed or re-architected?
- How do organizations cost-justify or assess the ROI of BC/DR solution(s)?
- Are organizations currently using disaster recovery-as-a-service (DRaaS) to protect servers and/or virtual machines (VMs)?
- What factors are driving organizations to consider cloud-based BC/DR services?

Survey participants represented a wide range of industries including financial services, manufacturing, business services, communications and media, and government. For more details, please see the *Research Methodology* and *Respondent Demographics* sections of this report.

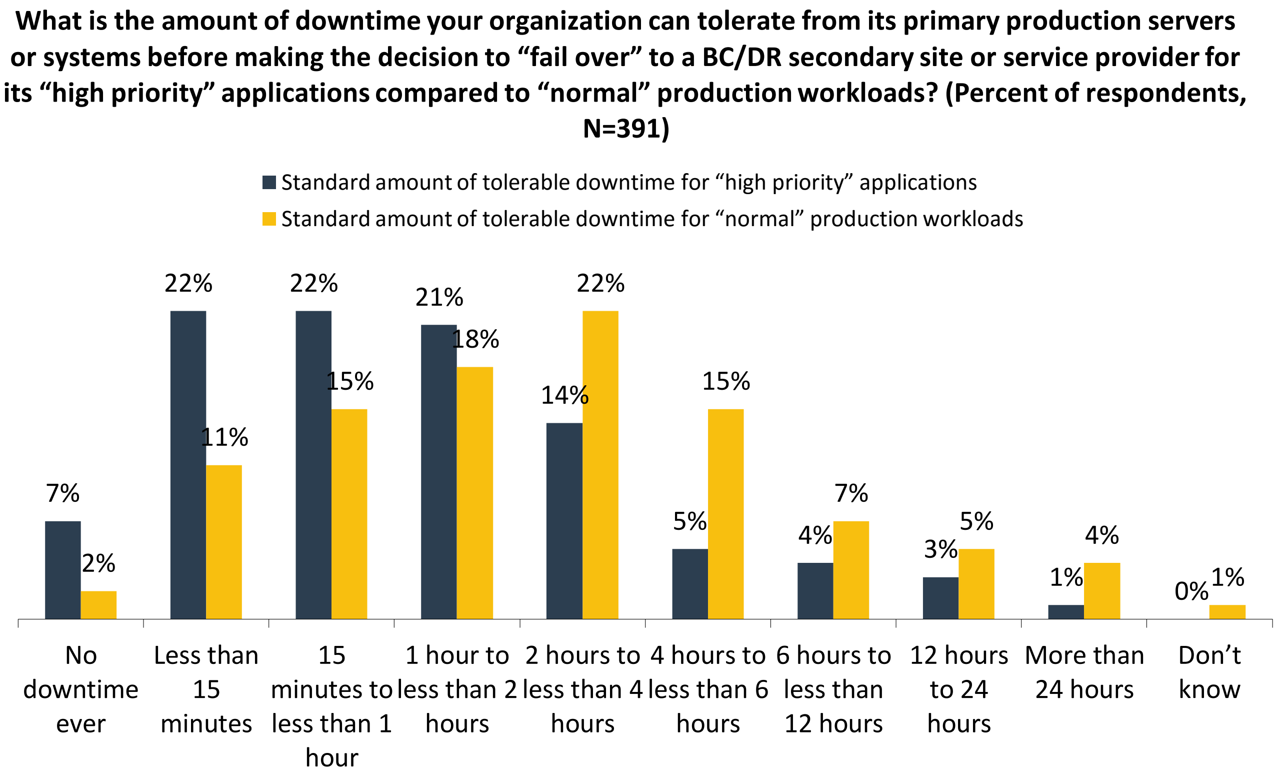
[1] Source: ESG Research Report, *2015 IT Spending Intentions Survey*, February 2015.

Research Findings

SLAs and Expectations

Any legitimate data protection discussion should begin around business continuity or disaster recovery. Figure 1 describes what amount of downtime can be tolerated by organizations before making the decision to “fail over” or invoke whatever recovery mechanisms are in place.

Figure 1. Amount of Downtime Organizations Can Tolerate for Primary Production Systems Before Failing Over to BC/DR Site: High Priority Applications vs. Normal Applications



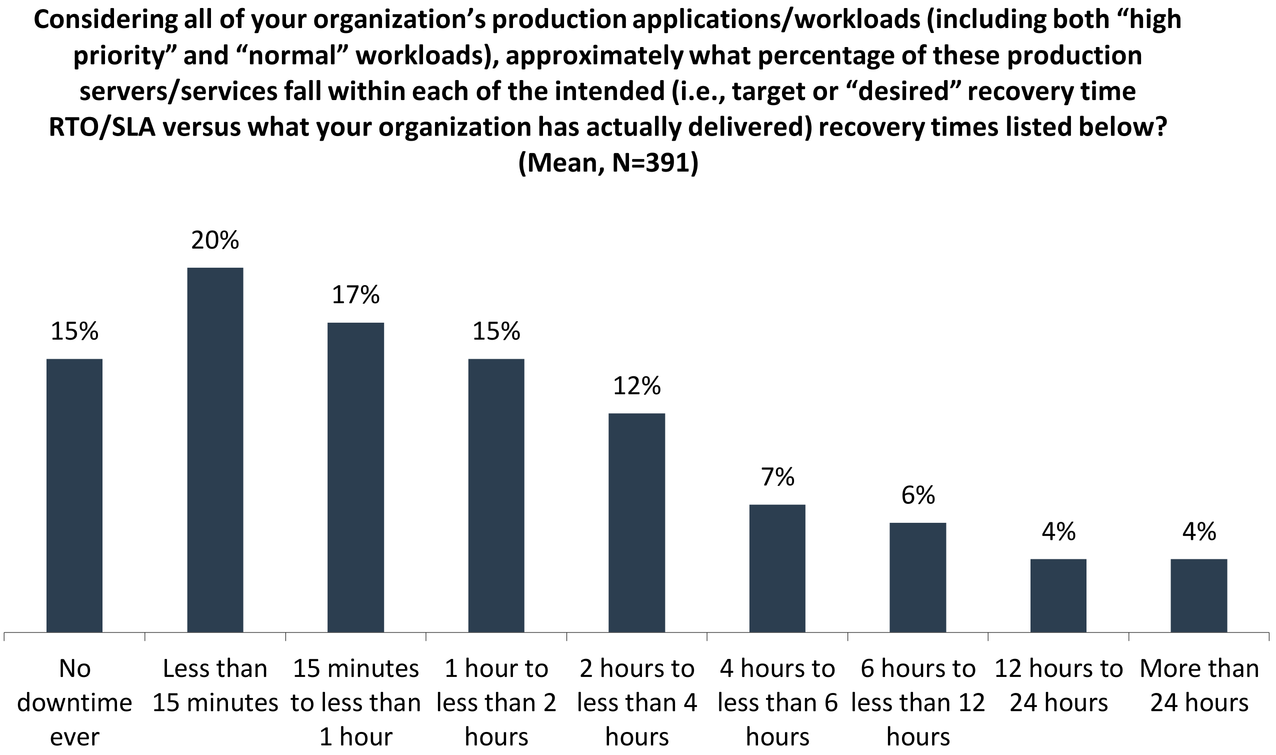
What is the amount of downtime your organization can tolerate from its primary production servers or systems before making the decision to “fail over” to a BC/DR secondary site or service provider for its “high priority” applications compared to “normal” production workloads? (Percent of respondents, N=391)

Source: Enterprise Strategy Group, 2016.

The challenge with Figure 1 is that it uses subjective terms such as “high priority” (also known as “tier-1” or “mission critical”) and “normal” to categorize the servers or applications prior to defining their tolerance to downtime. This strategy has historically been used by IT organizations, whereby high priority platforms would receive whatever heroics or atypical data recovery mechanisms that were available within the organization, while the normal platforms or “everything else” would simply be protected by nightly backup operations. Unfortunately, this can lead to misunderstandings and over-/under-protection based on whether the subjective monikers are applied to the top 5% or top 30% of the IT infrastructure.

To provide clarity in this regard, ESG asked a similar question on “intended recovery times” across the organization, whereby respondents could quantify what percentage of their infrastructure fell under each recovery goal, as seen in Figure 2.

Figure 2. Percentage of Production Servers/Services that Fall Within Each of the Intended Recovery Times



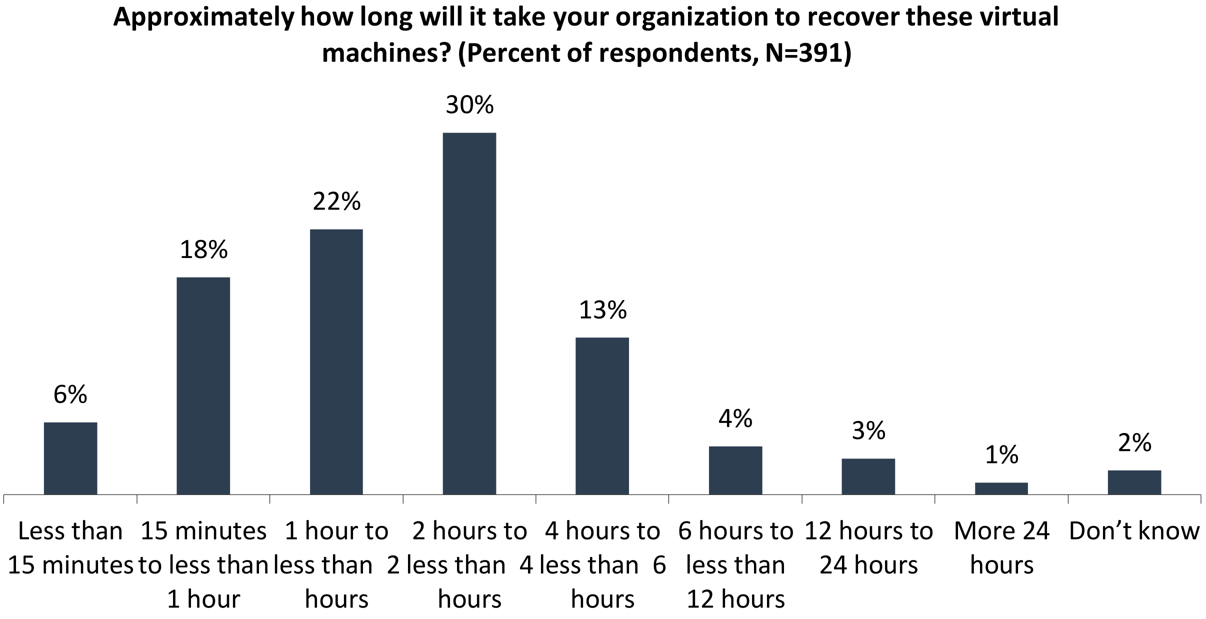
Source: Enterprise Strategy Group, 2016.

Figure 2 is perhaps one of the most important charts in this report, revealing the criticality of the vast majority of servers across the IT environment, most of which cannot be addressed by traditional backup alone:

- *More than one-third (35%) have a recovery goal of 15 minutes or less*, which is arguably not addressable by any reactive recovery mechanism, including backups, snapshots, and replication. Instead, proactive **high-availability or failover technologies** should be considered.
- *Nearly a third (32%) have a recovery goal between 15 minutes and two hours*, where **replicas/snapshots** are inarguably best suited; though some **"rapid" or "instant" VM recovery features** may also be applicable.
- *Another fifth (19%) have a recovery goal between 2 and 6 hours*, where **modern backup and restoration** are more applicable—with features like rapid/instant VM recovery and snapshot/replica-integration to backups being differentiable and desirable features.
- This leaves *only 14% recovery goals greater than six hours*, where mediocre or legacy backup mechanisms may be "good enough."

While Figure 1 and Figure 2 depict downtime tolerance and intended RTO/SLAs for recoverability, Figure 3 shows the reality of how long it takes for IT respondents to actually recover a VM, which, in most environments, is faster than recovering physical servers. Even as a best case (VMs versus physical servers), the actual recovery times found in Figure 3 are insufficient compared with the downtime tolerances and desired SLAs described earlier.

Figure 3. Length of Time Needed to Recover Virtual Machines



Source: Enterprise Strategy Group, 2016.

The comparison of reality (Figure 3) with the desired SLAs (Figure 2) and downtime tolerances (Figure 1) tells a very clear story: Backup alone isn’t enough. For many environments, even modern backups with fast recoveries are insufficient, driving the need for a broader strategy of data protection that also includes snapshots and replication. But to really address the dependencies that business units have on their IT resources, a broader approach for data protection that includes proactive high availability and business continuity mechanisms should be part of a comprehensive approach to IT.

BC/DR Mechanisms

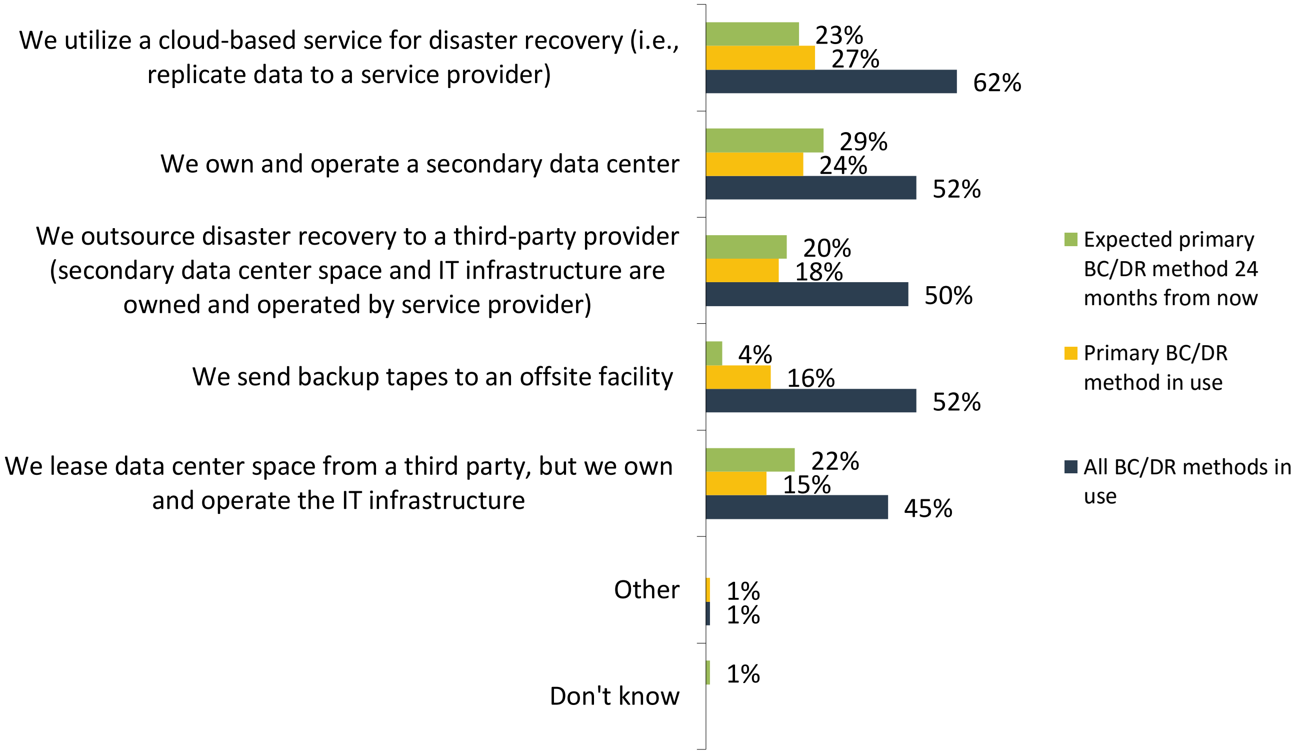
Addressing the strategic aspects of data protection through business continuity and disaster recovery mechanisms can be daunting, considering the myriad methods of BC/DR that are available to IT organizations today, as seen in Figure 4.

Figure 4 tells two stories in parallel:

- Many organizations use multiple mechanisms as part of their BC/DR strategy. Said another way, each of the methods described above is in use in roughly half of environments.
- The top two methods, comprising just over half of respondents, are relatively balanced between those using a cloud service as their primary means of BC/DR and those using a self-managed BC/DR site as their primary method; with similar anticipated usage over the next two years, albeit with some shift in approach.

Figure 4. Methods Used as Part of Disaster Recovery Strategy

Which of the following methods are used as part of your organization's disaster recovery strategy? Which would you identify as your organization's primary (as determined by the method providing resiliency to the greatest percentage of recoverable servers) disaster recovery method? Which do you believe will be your organization's primary disaster recovery process in 24 months? (Percent of respondents, N=391)

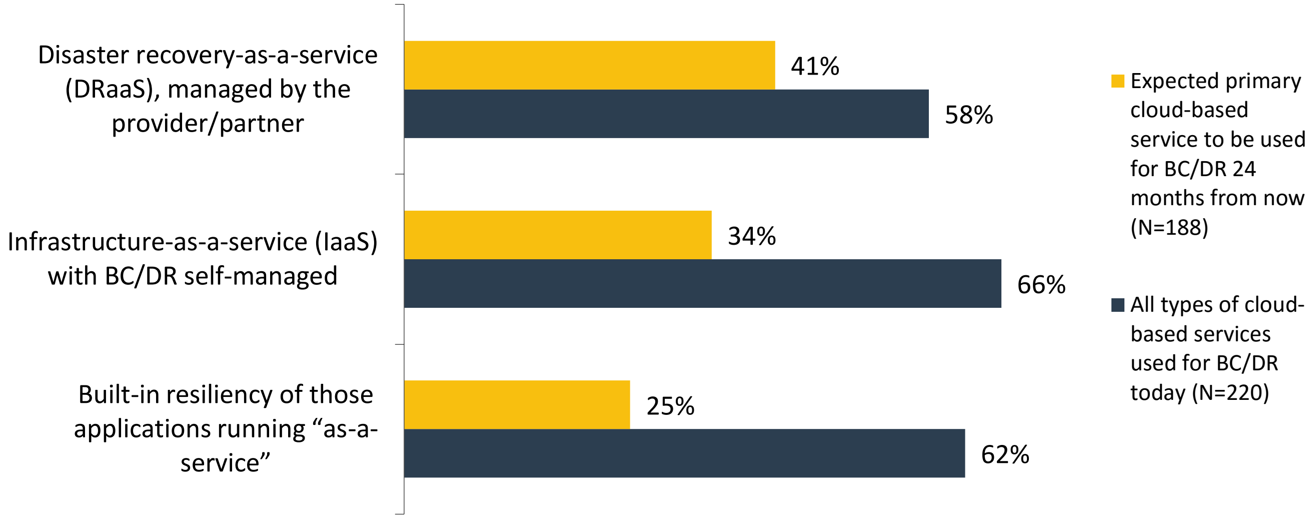


Source: Enterprise Strategy Group, 2016.

To be clear, the leading primary method of using a "cloud service" in Figure 4 can be interpreted in multiple ways, including DRaaS, cloud-based secondary infrastructure-as-a-service (IaaS), or a natively resilient production cloud service (thus mitigating the need for failover/availability of those services). The question of which types of cloud services are used in support of BC/DR goals is addressed in Figure 5.

Figure 5. Cloud Services Used for BC/DR: Today and 24 Months from Now

Which types of cloud services does your organization utilize for BC/DR today? Which method do you anticipate being your organization's primary cloud-mechanism for BC/DR 24 months from now? (Percent of respondents)

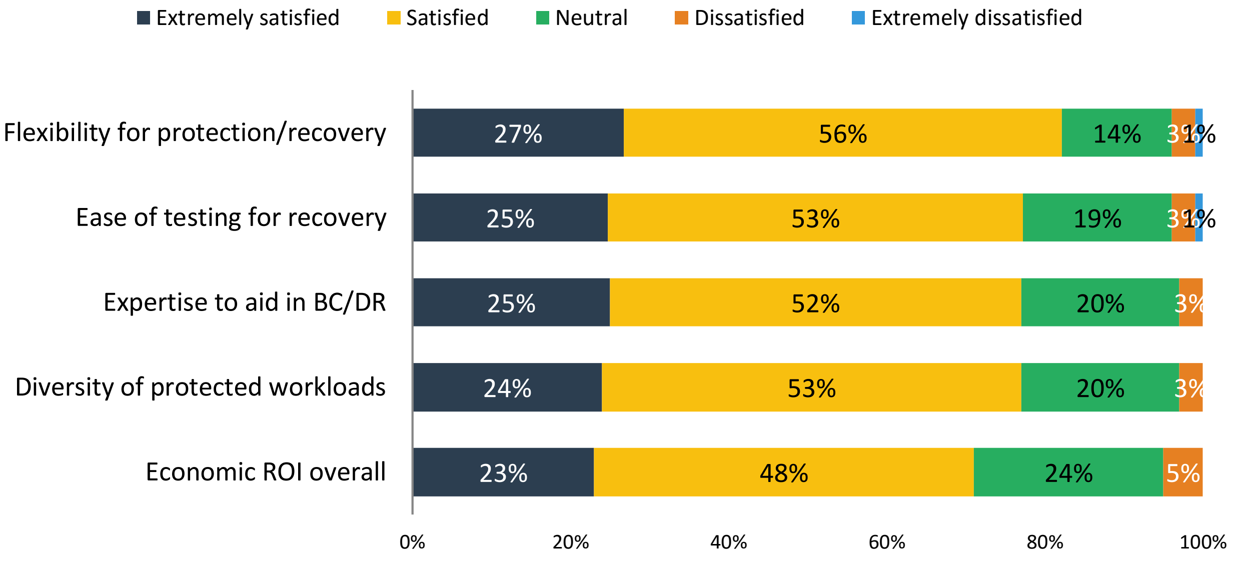


Source: Enterprise Strategy Group, 2016.

To explore beyond the actual usage of the various means of BC/DR, Figure 6 shows the mostly positive (though not overwhelming) opinion of the primary BC/DR method (which was measured in yellow in Figure 4).

Figure 6. Opinions on Current Primary BC/DR Facility

Considering your organization's primary BC/DR site or service today, please rate it on the following criteria: (Percent of respondents, N=391)

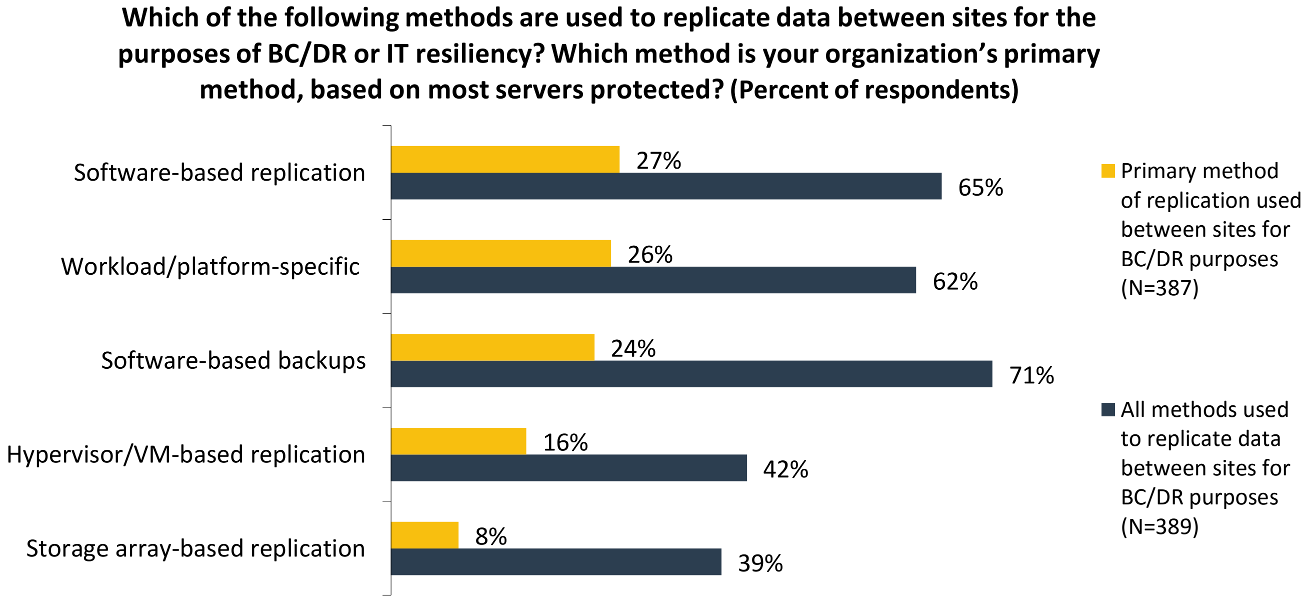


Source: Enterprise Strategy Group, 2016.

BC/DR Technologies

Digging beyond the BC/DR facilities or services used, ESG also explored what technologies were used to replicate the data between sites as part of BC/DR preparedness (see Figure 7).

Figure 7. Summary of Methods Used to Replicate Data Between Sites for BC/DR



Source: Enterprise Strategy Group, 2016.

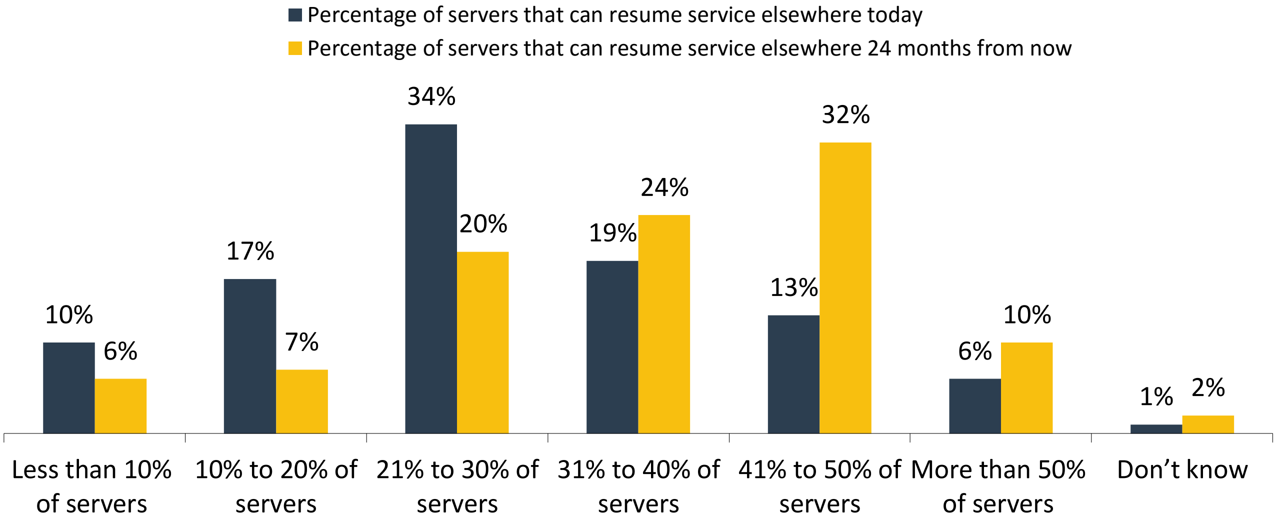
After ensuring one or more redundant copies of data for BC/DR, as shown above, Figure 8 shows the actual percentage of servers with the ability to fail over (resume functionality) today, as well as the projected percentage two years from now. According to Figure 8, the average organization reports that 28% of their production servers can fail over today, which is expected to increase to 35% within two years. ESG expects this number to rise as:

- The affordability of BC/DR technologies increases
- The awareness of SLAs and organizations' inability to meet them increases.
- The complexity of BC/DR technologies and hybrid infrastructures becomes less overwhelming.

Figure 9 brings together the various replication methods and ability to fail over within a single lens, with a breakdown of approaches used for physical servers compared with virtual machines.

Figure 8. Percentage of Production Servers with the Ability to Resume Functionality at a BC-DR Site/Service: Today and 24 Months from Now

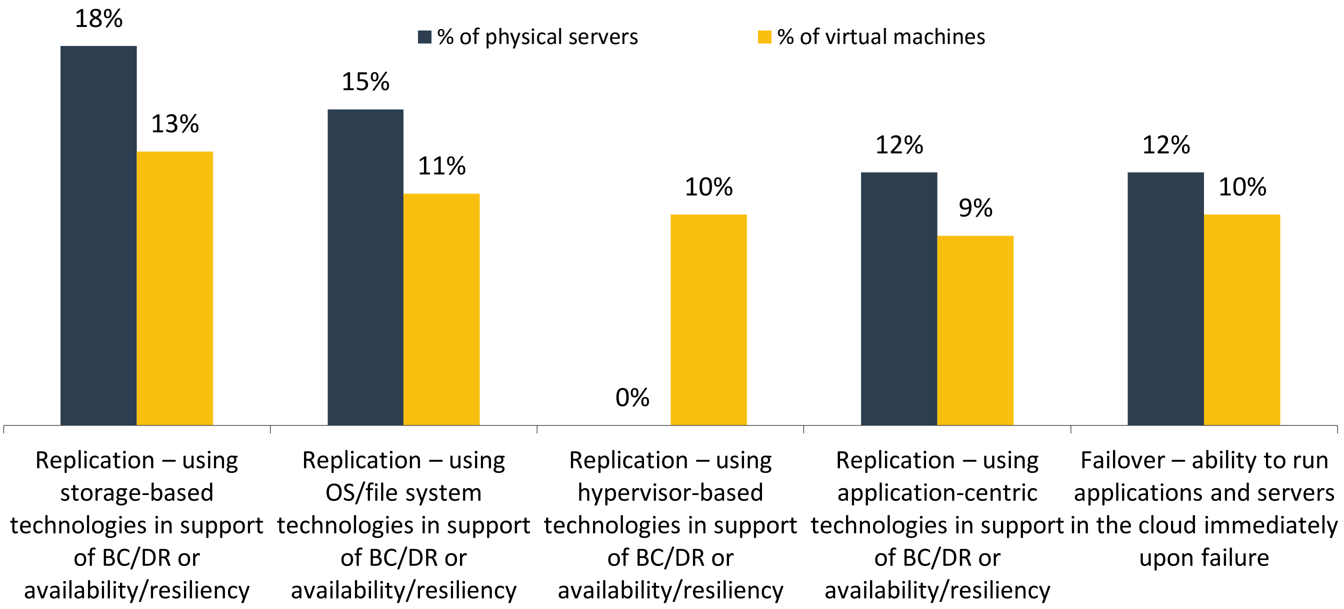
Of all the production servers used by your organization, approximately what percentage is currently able to resume functionality at a secondary BC/DR site or service of some kind? How do you expect this to change over the next 24 months? (Percent of respondents, N=391)



Source: Enterprise Strategy Group, 2016.

Figure 9. Percentage of Production Physical Servers and Virtual Machines with the Data Protection Activities Being Applied

For each of the following data protection activities, please indicate the approximate percentage of your organization's production physical servers (not including virtualization hosts) and virtual machines that have those technologies being applied to them today. (Mean, N=391)



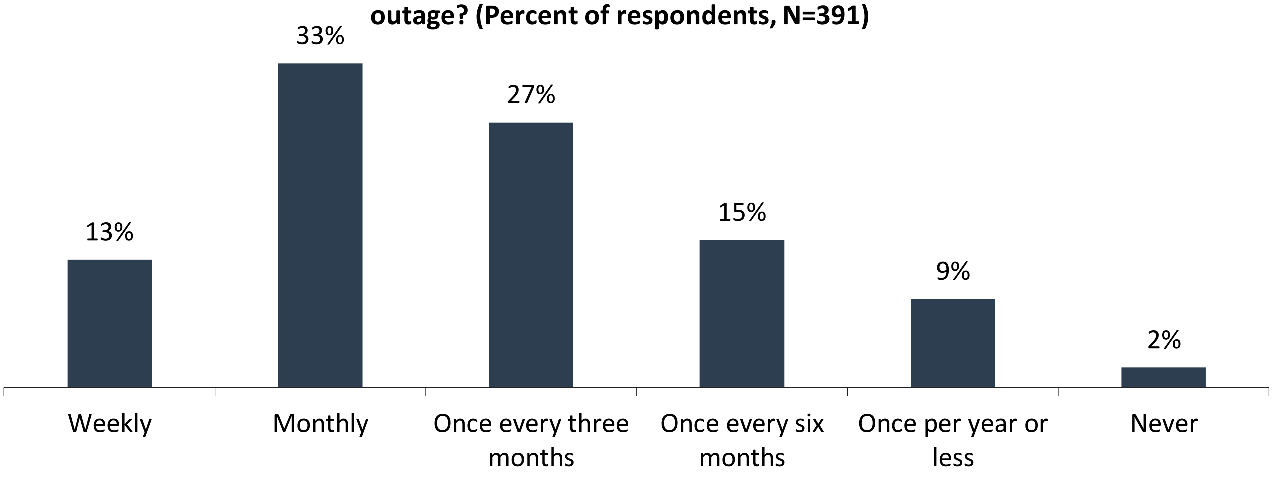
Source: Enterprise Strategy Group, 2016.

BC/DR Testing Frequency and Methodology

As it is often stated, BC/DR is about more than the replication technologies that ensure data survivability. Key among BC/DR processes is testing, whose frequency is measured in Figure 10. It is worth noting that the testing frequency shown in Figure 10 is appreciably higher than the test frequency seen in ESG's 2013 *Data Protection-as-a-service (DPaaS) Trends* research.

Figure 10. Frequency of Executing a Test Recovery

How often does your organization execute a test recovery to determine if/how quickly it can recover from its BC/DR site or service provider systems in the event of an outage? (Percent of respondents, N=391)



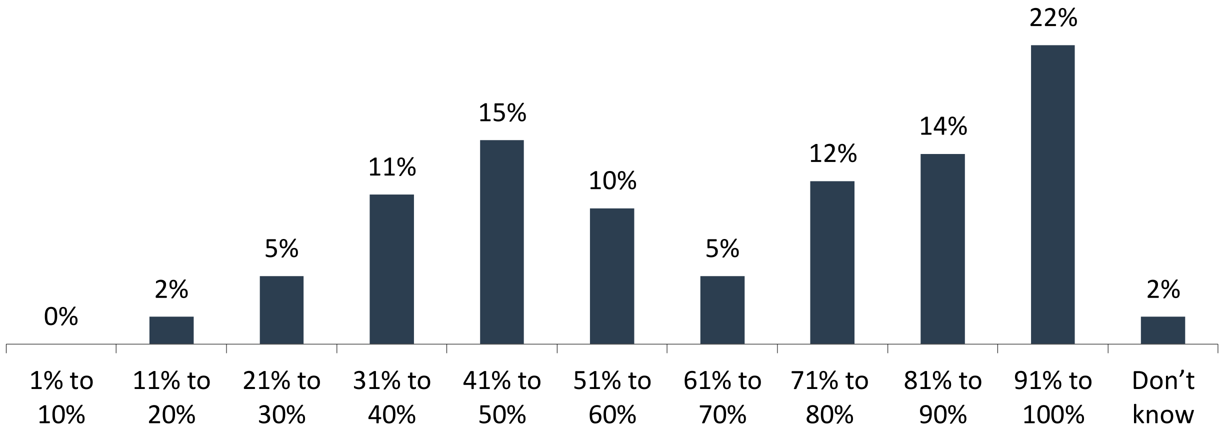
Source: Enterprise Strategy Group, 2016.

Equally as important as the frequency of BC/DR test is the mindset for "passing" or "failing" those tests, as seen in Figure 11. Among the organizations that do test their BC/DR processes, the rough average success rate is 65%, which can be taken in two ways, depending on your mindset:

- If you test BC/DR looking for "green checkmarks," you will likely under-test, which could result in the inability to recover when you really need it.
- If you test BC/DR looking for "red Xs," you will likely find opportunities to improve, thereby increasing your ability to recover when necessary.

Figure 11. Percentage of BC/DR Tests that Succeed

On average, approximately what percentage of your organization's routine tests for BC/DR preparedness succeed or "pass"? (Percent of respondents, N=383)



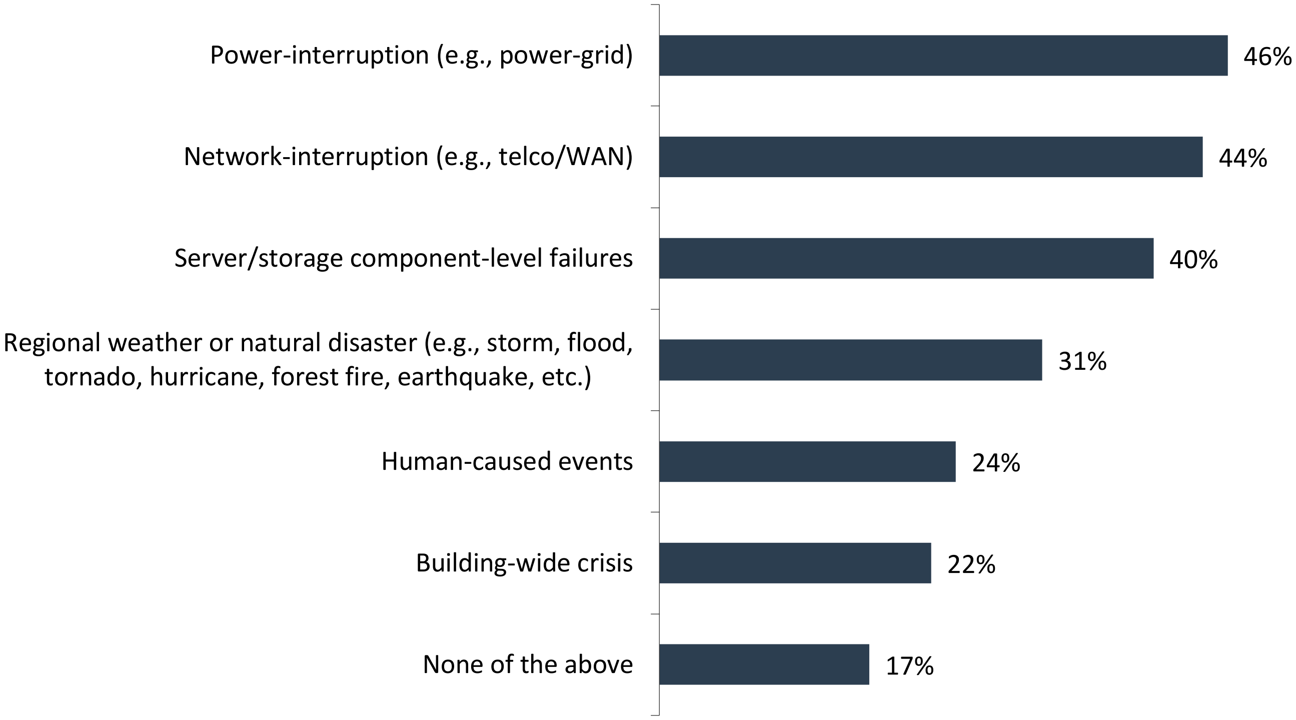
Source: Enterprise Strategy Group, 2016.

BC/DR Invocation Frequency and Causes

Beyond the frequency of testing is the actual frequency of using one's BC/DR capabilities, as well as understanding the causes involved. While it may surprise some, wide-scale regional events (such as weather) are not the main triggers for failing over the BC/DR resource pool. Instead, Figure 12 shows that "connectivity issues" of power or networking are actually the main causes of impedance requiring mitigation.

Figure 12. BC/DR Events that Caused Organizations to Leverage a Secondary Site in the Last Two Years

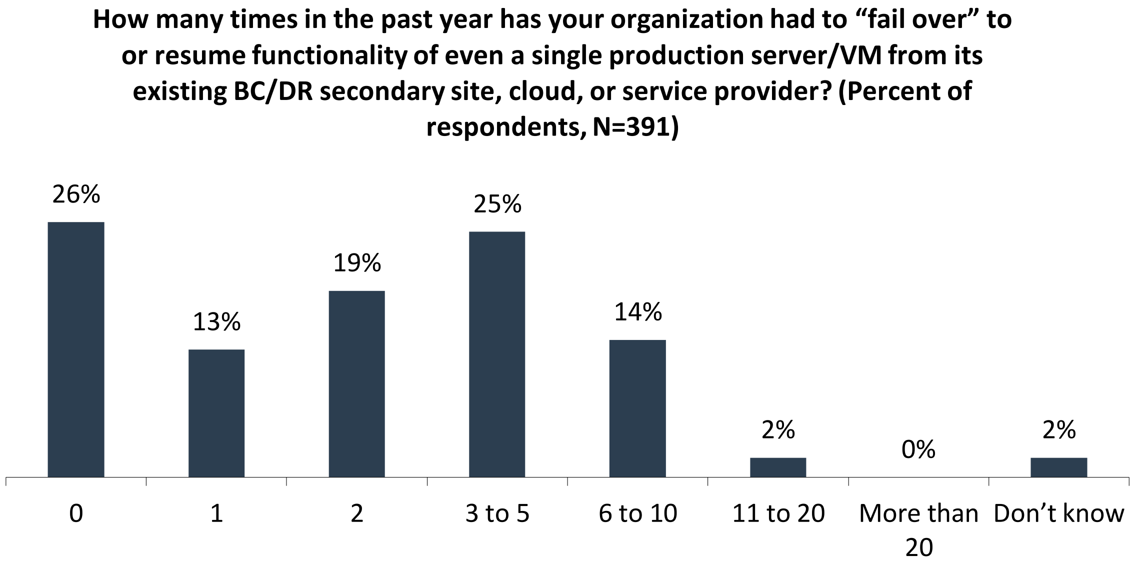
In the last two years, which types of BC/DR event–if any–caused your organization to leverage a secondary site or infrastructure as part of its IT recovery experience? (Percent of respondents, N=391, multiple responses accepted)



Source: Enterprise Strategy Group, 2016.

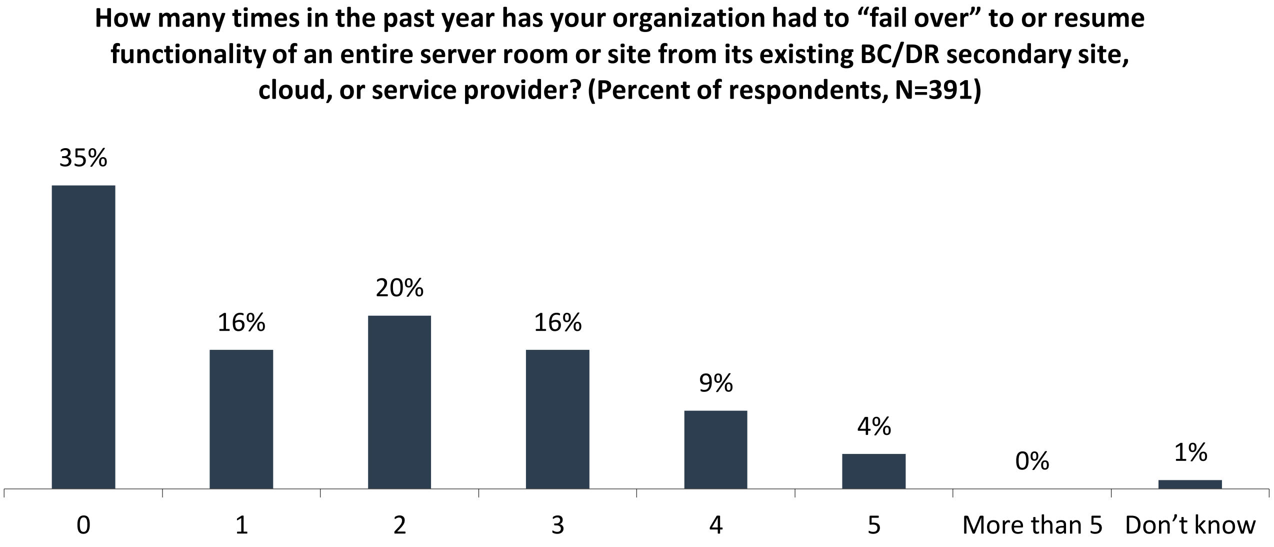
With connectivity issues (Figure 12) topping the list of what causes failover, Figure 13 shows the frequency of a single VM or server being failed over.

Figure 13. Number of Times in the Past Year Organizations Had to "Fail Over" to or Resume Functionality of a Production Server/VM *from Existing BC/DR Site, Cloud, or Service Provider*



Source: Enterprise Strategy Group, 2016.

Figure 14. Number of Times in the Past Year Organizations Had to "Fail Over" to or Resume Functionality of an Entire Server Room or Site *from Existing BC/DR Site, Cloud, or Service Provider*

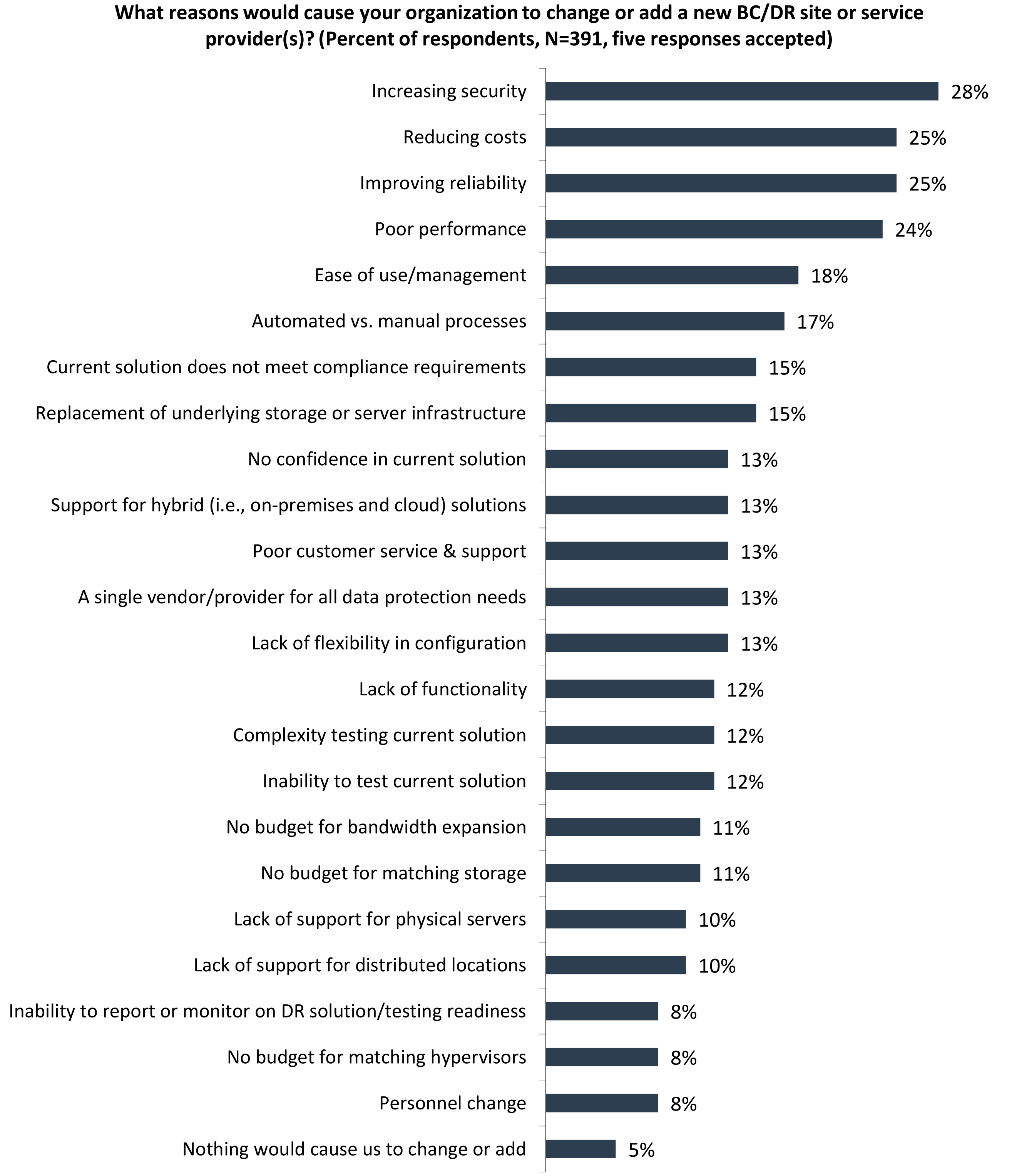


Source: Enterprise Strategy Group, 2016.

BC/DR Considerations and Perceptions toward Providers and Services

As seen in Figure 15, the top considerations that would influence changing or adding a new BC/DR provider include the same kinds of top drivers found in ESG's *2015 Trends in Data Protection Modernization* research concerning change considerations around security, cost, and reliability/performance.

Figure 15. Factors that Would Influence Change of BC/DR Site or Service Provider

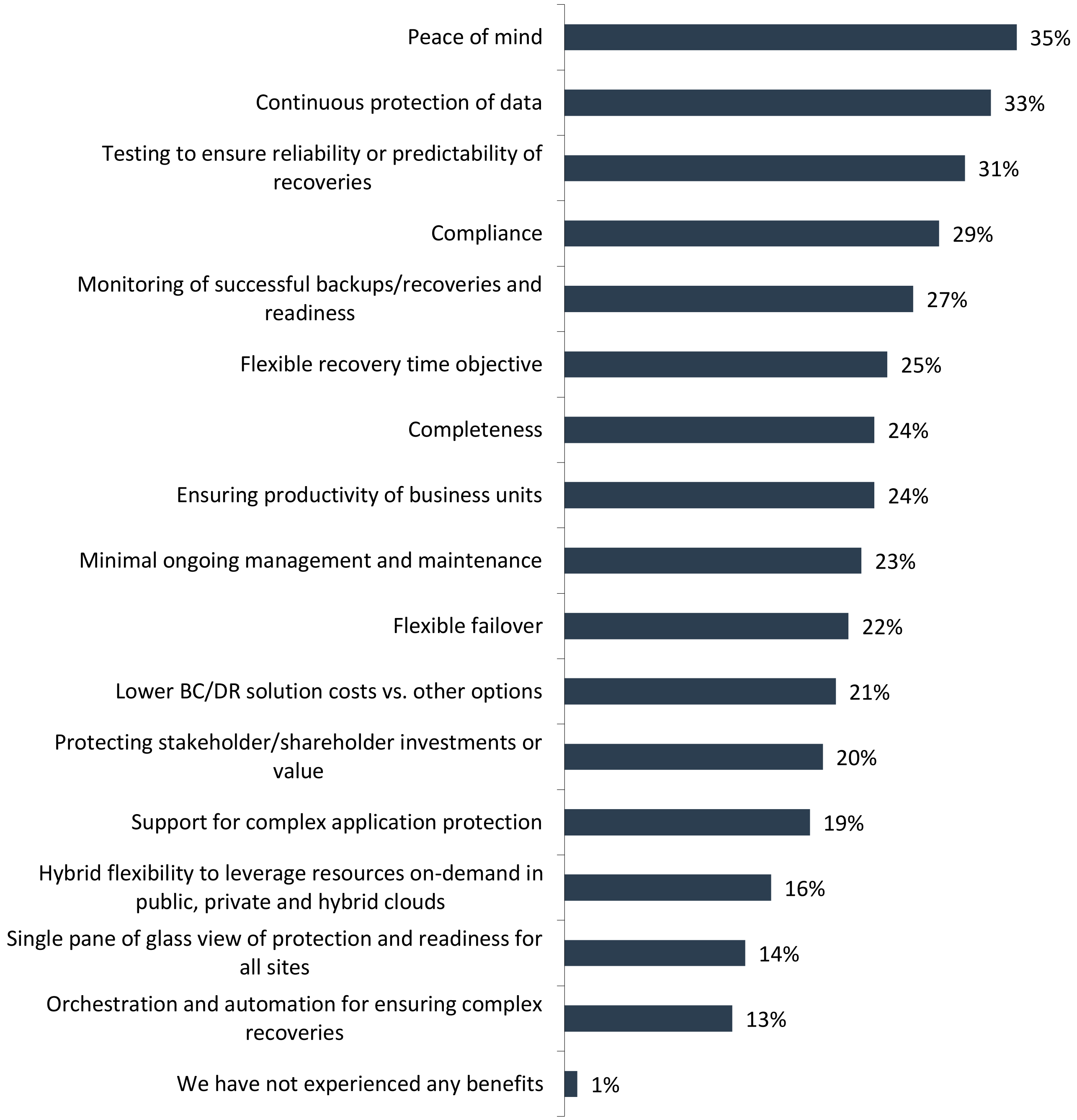


Source: Enterprise Strategy Group, 2016.

While Figure 15 shows considerations from a forward-facing perspective, Figure 16 gives a retrospective view on the top benefits gained from current BC/DR solutions.

Figure 16. Benefits Gained from BC/DR Site or Service Provider

What are the top benefits that your organization gains from its current BC/DR site or service provider? (Percent of respondents, N=391, five responses accepted)



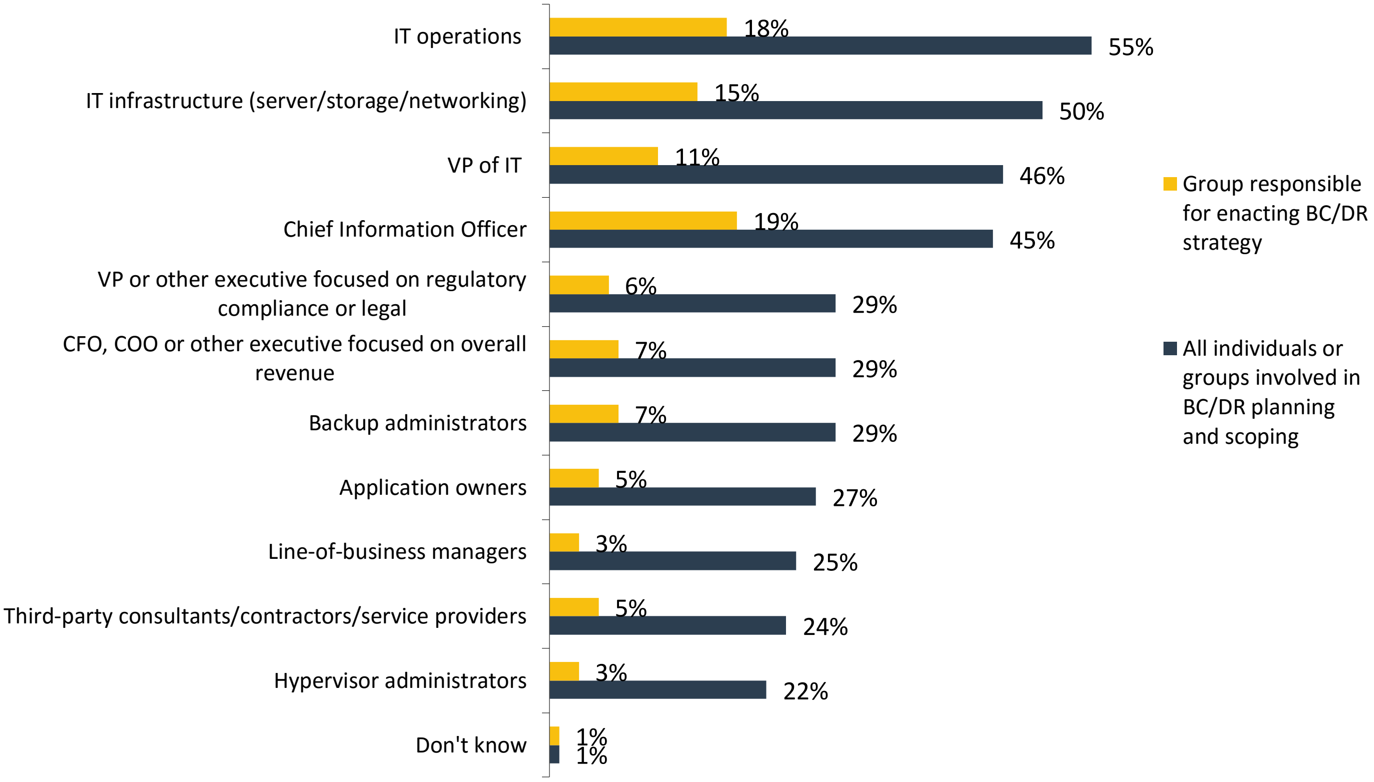
Source: Enterprise Strategy Group, 2016.

BC/DR Personnel, Strategies, and Tools

BC/DR is as much about corporate culture and process as it is about technology—though without one's data, most of the culture/process won't matter. That being said, to really affect culture and process takes much more than a traditional backup administrator can accomplish. Figure 17 shows all of the role types involved in BC/DR planning (blue), as well as the groups/individuals responsible for enacting the strategy (yellow).

Figure 17. Roles/Groups Involved in Planning and Enacting BC/DR Strategy

What roles or groups are actively involved in planning and scoping out your organization's BC/DR strategy? Which group is ultimately charged with enacting the BC/DR strategy, if necessary? (Percent of respondents, N=391)

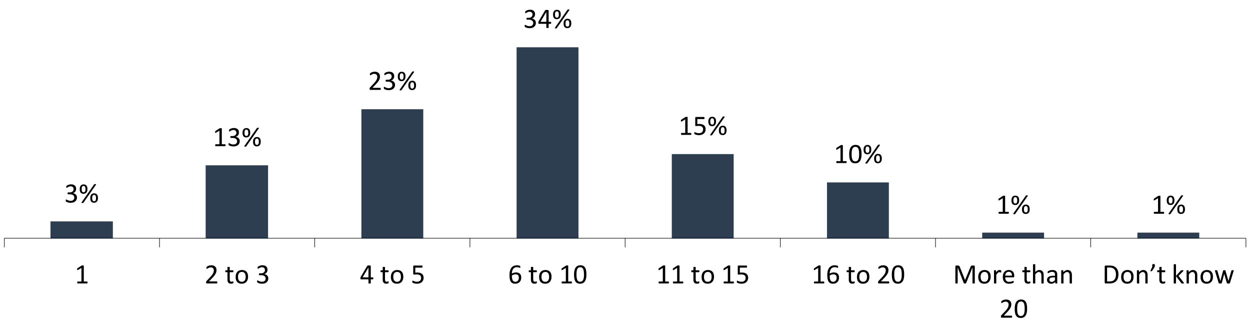


Source: Enterprise Strategy Group, 2016.

As a follow-on to the types of roles involved in or driving the process, Figure 18 shows the BC/DR team size.

Figure 18. Number of Individuals Involved in Planning and Scoping BC/DR Strategy

Approximately how many total individuals are actively involved in planning and scoping out your organization's BC/DR strategy? (Percent of respondents, N=391)

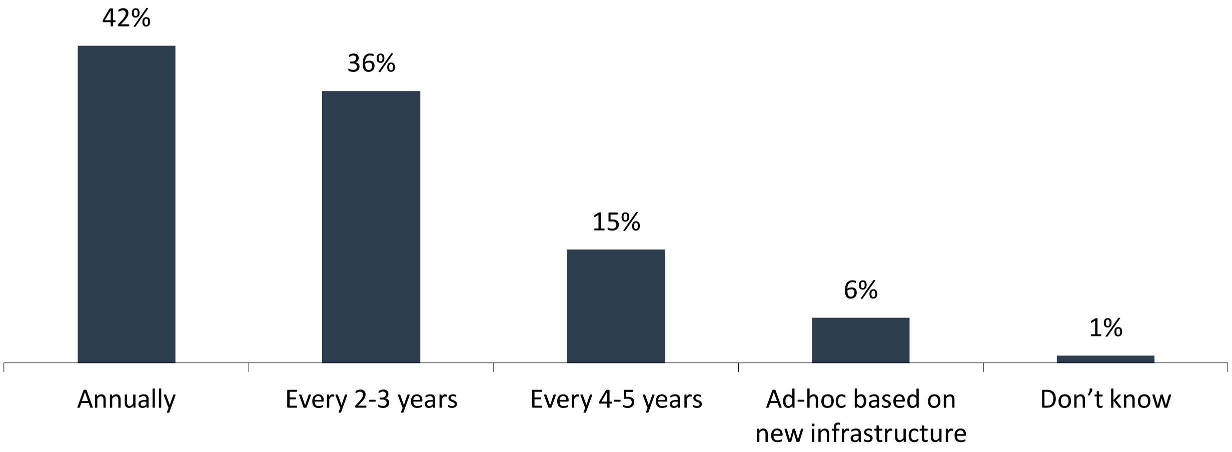


Source: Enterprise Strategy Group, 2016.

The BC/DR groups and individuals have the ongoing task of planning, implementing, testing, and reevaluating for continuous improvement. According to Figure 19, a plurality of respondents (42%) indicate an annual cadence for their organization's BC/DR strategy assessments, though the rough extrapolated average for those indicating a recurring quantity (i.e., *not* ad-hoc) works out to a little more than two years.

Figure 19. Frequency of BC/DR Strategy Development

How frequently is your organization's BC/DR strategy assessed or re-architected? (Percent of respondents, N=391)

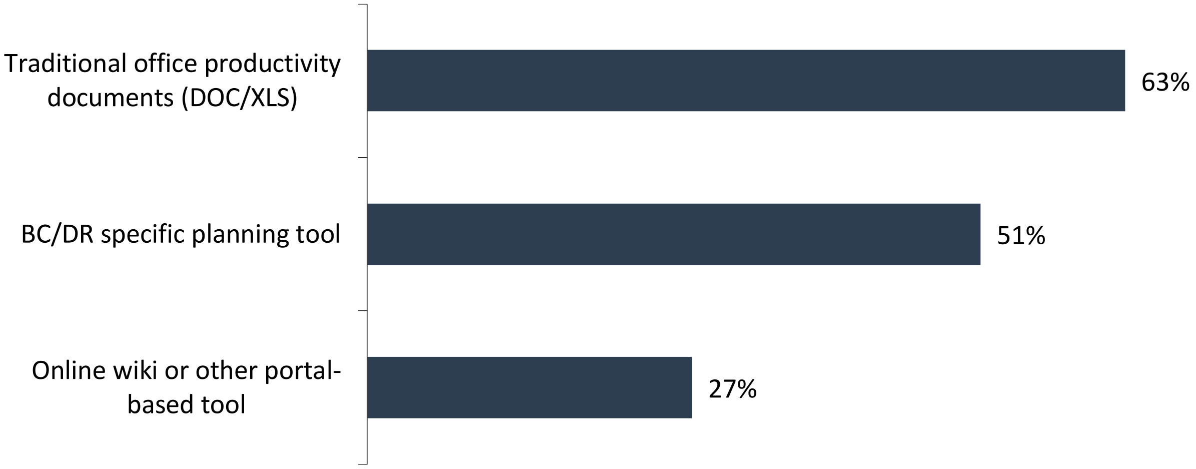


Source: Enterprise Strategy Group, 2016.

As seen in Figure 20, the BC/DR plan can be developed or maintained in a variety of ways, which may be of particular interest to vendors whose data protection technologies have the ability to report to or be invoked from an outside tool or interface, such as (potentially) the BC/DR planning interface.

Figure 20. Tools Used to Develop or Maintain BC/DR Plan

What tool(s) does your organization use to develop or maintain its BC/DR plan? (Percent of respondents, N=391, multiple responses accepted)

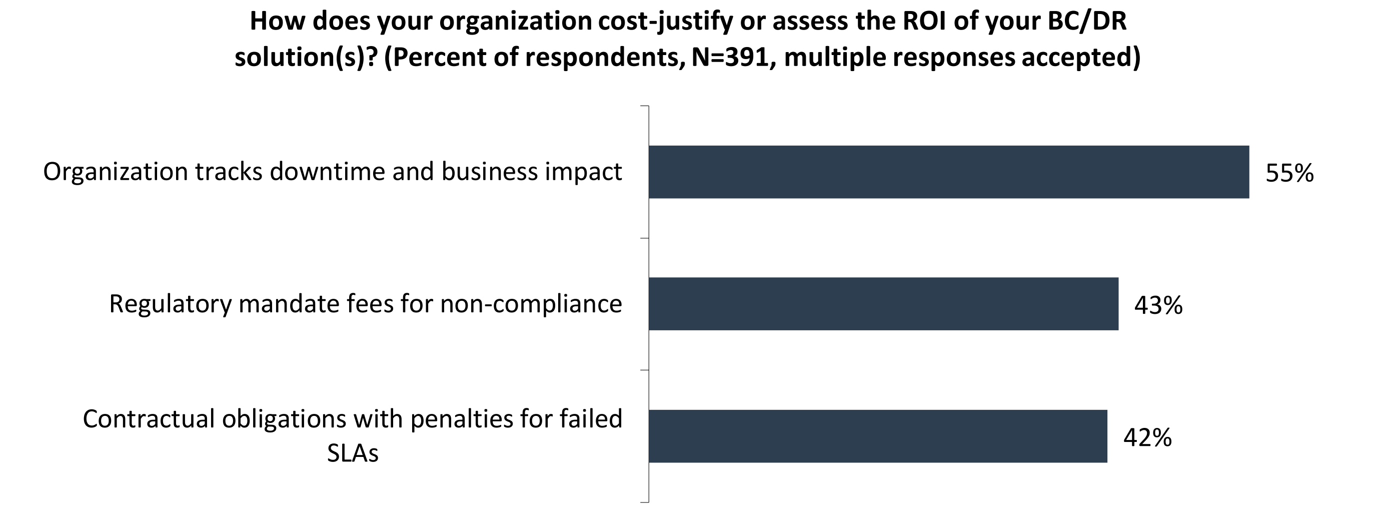


Source: Enterprise Strategy Group, 2016.

BC/DR Economics

For many organizations, while everyone instinctually recognizes the importance of BC/DR, based on an awareness of dependency on IT, it can be hard to quantify the actual ROI of the investments in BC/DR. This should not imply that the cost of downtime is negligible. The cost of downtime is exorbitantly higher than most organizations realize, but is often too complex to accurately quantify per user, per VM, or per physical host/server. That being said, more than half (55%) of respondent organizations track the downtime and associated business impact in order to justify the value of their BC/DR solutions (see Figure 21).

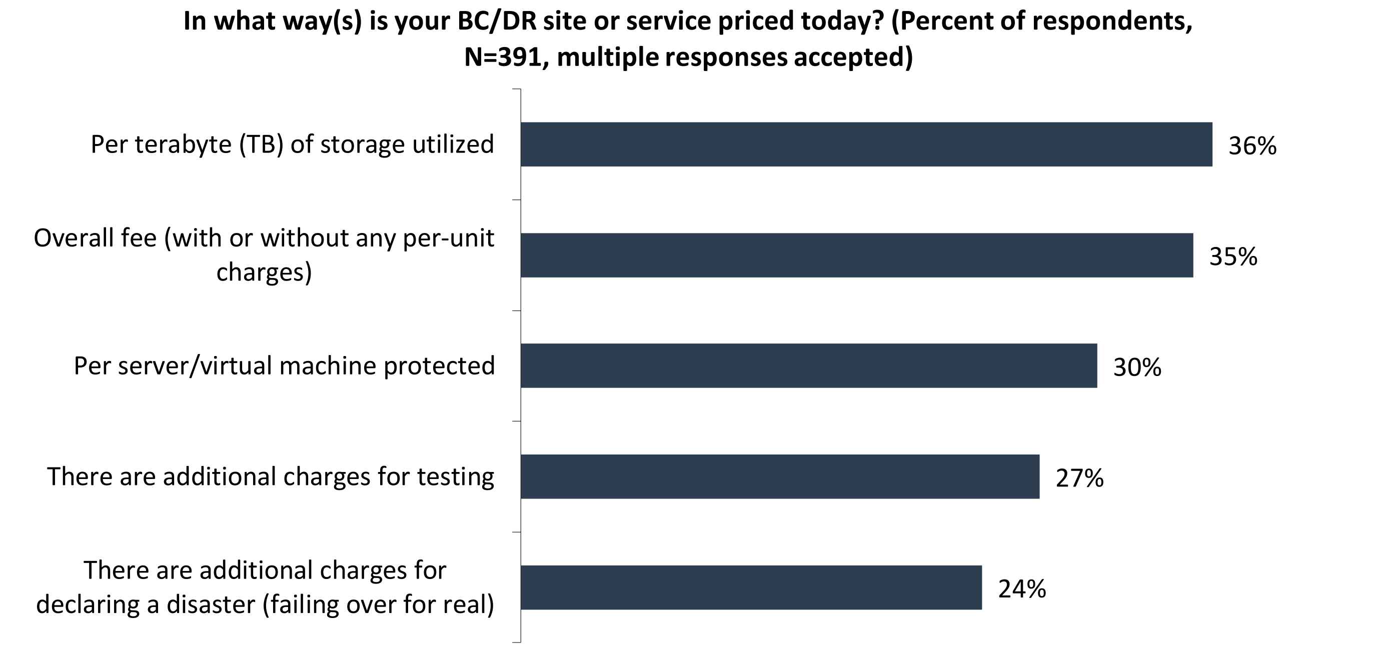
Figure 21. How Organizations Assess the ROI of BC/DR Solution(s)



Source: Enterprise Strategy Group, 2016.

Part of the challenge of calculating the ROI of BC/DR is comparing the business impact of outages with what can be a complex cost structure for BC/DR, as seen in Figure 22.

Figure 22. How BC/DR Site or Service Is Priced Today



Source: Enterprise Strategy Group, 2016.

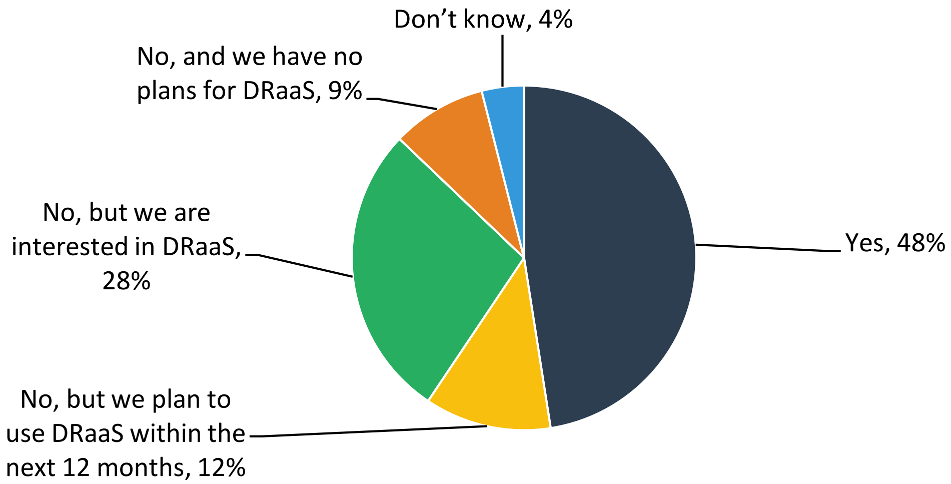
Disaster Recovery-as-a-service (DRaaS)

Usage Trends and Drivers

One of the most interesting BC/DR alternatives in market the today is disaster recovery-as-a-service (DRaaS), whereby production resources fail over to cloud-based resources. According to Figure 23, nearly half of all organizations are utilizing a DRaaS solution to protect servers/VMs *in some way*.

Figure 23. Current Use of DRaaS to Protect Servers and/or VMs

Is your organization currently using disaster recovery-as-a-service (DRaaS) to protect any of its servers and/or virtual machines (VMs)? (Percent of respondents, N=391)

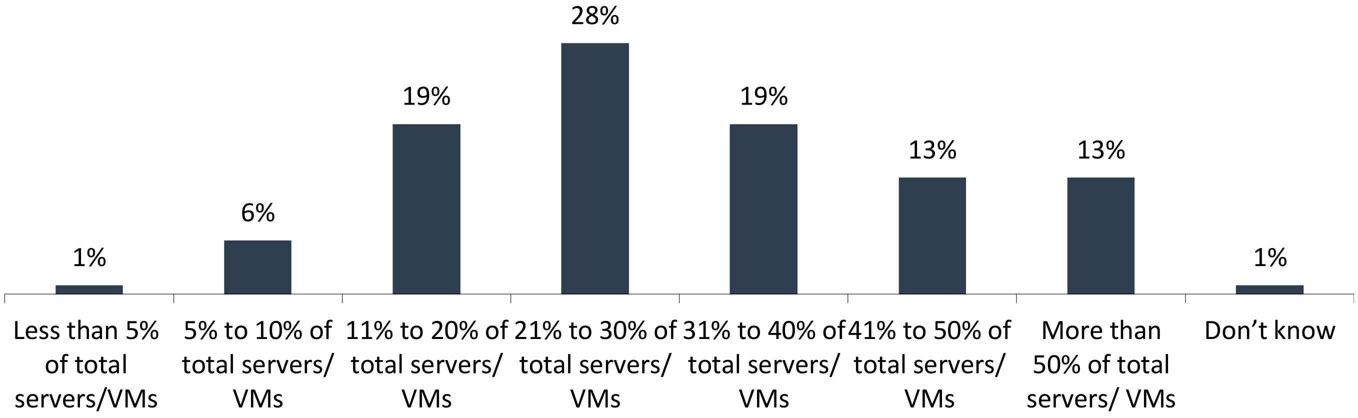


Source: Enterprise Strategy Group, 2016.

To be clear, the data does not show DRaaS as the *primary* means of recovery for nearly half of all organizations, only that it is used in *some* way to protect *any* of their servers or VMs. In fact, Figure 24 shows that–on average–organizations protect–or expect to protect–nearly one-third of their virtual and physical servers using DRaaS.

Figure 24. Percentage of Servers or VMs Currently—or Likely To Be—Protected by a Cloud-based DR Service

Approximately what percentage of your organization's total servers or virtual machines would you estimate is currently – or likely will be – protected to a cloud-based disaster recovery service? (Percent of respondents, N=342)

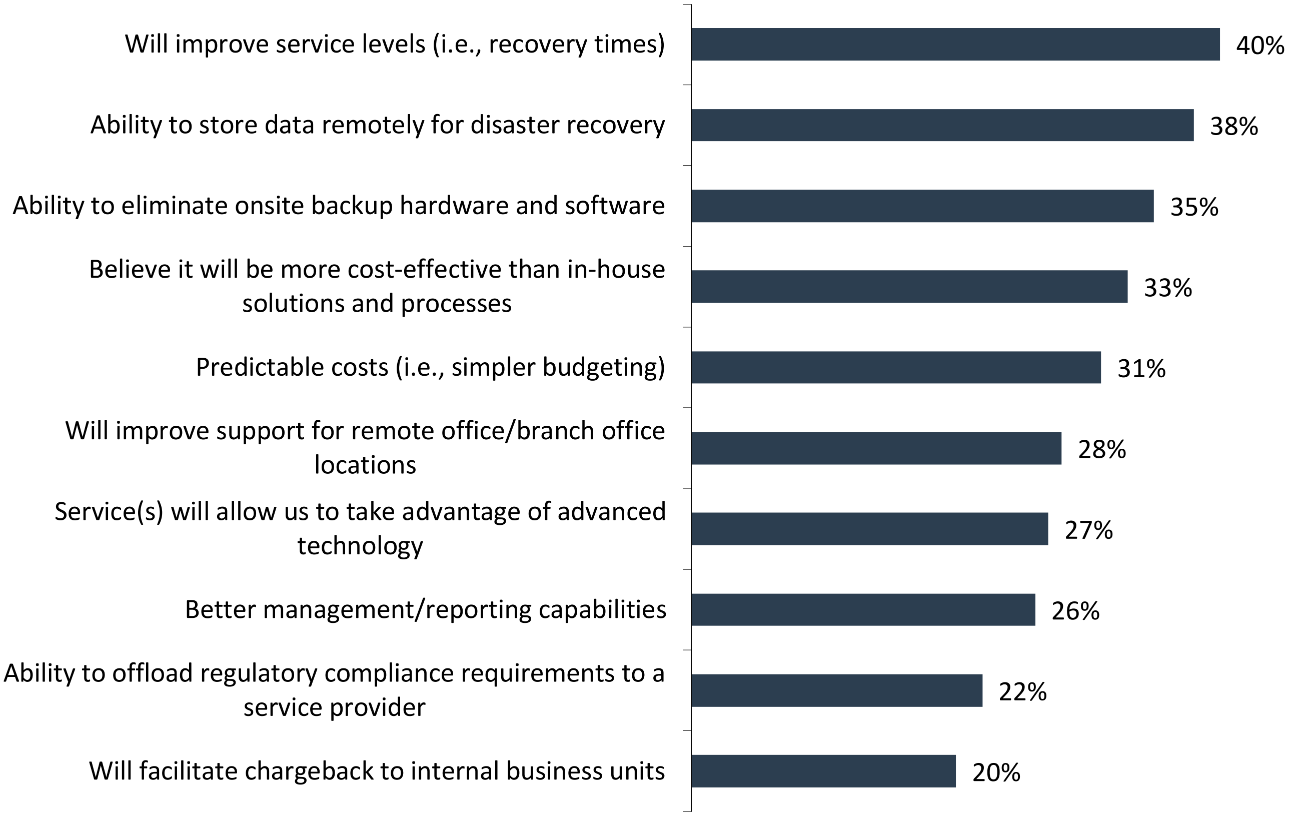


Source: Enterprise Strategy Group, 2016.

For those considering DRaaS, Figure 25 shows the factors driving DRaaS adoption.

Figure 25. Factors Driving Consideration of Cloud-based BC/DR Services

Which of the following factors is driving your organization to consider cloud-based BC/DR services? (Percent of respondents, N=142, multiple responses accepted)



Source: Enterprise Strategy Group, 2016.

DRaaS Preferences of Providers and Features

One of the key considerations for DRaaS is who IT organizations partner with to achieve their BC/DR preparedness, which is arguably more important than the technology in use or where the data resides. Figure 26 shows an interesting trend in the preferred purchasing sources for DRaaS solutions.

The general trend around the convergence of *expertise* and *capability* reflected in Figure 26 was observed in similar 2013 DRaaS trends research.[2] These findings include:

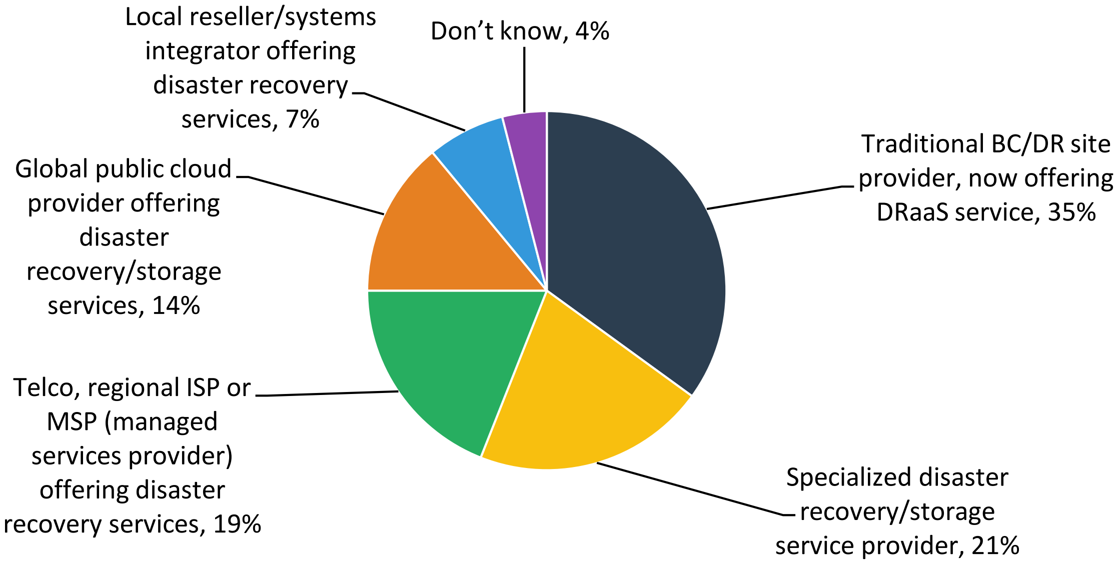
- The least desired (7%) DRaaS provider is the **local partner**, which may be counter-intuitive considering that the partner has the most insight or empathy for the customer environment and would likely be among the first resources called during a crisis. Notwithstanding the concern that a local partner may be suffering from the same local/regional crisis as the customer, the broader rationale gleaned in 2013 interviews was concern over the partner's capability to run a reliable and secure secondary infrastructure.[3]
- The next two categories, including **global public cloud provider** (14%) and **regional telco/MSP** (19%), have the opposite challenge: They can run a reliable and secure secondary infrastructure, but likely do not have empathy for the customer environment or BC/DR planning expertise.
- It isn't until we see the proven convergence of experience (in BC/DR planning and awareness of the customer's recovery needs) and capability (to run a reliable and secure secondary infrastructure) that we see the most customer interest, which includes the use of **specialized DR services** (21%) and **traditional BC/DR providers** that are now offering DRaaS (35%).

[2] Source: ESG Research Report, *Data Protection-as-a-service (DPaaS) Trends*, September 2013.

[3] ibid.

Figure 26. Preferred Provider(s) of DRaaS

From which of the following sources does your organization purchase – or expect to purchase – a DRaaS solution? (Percent of respondents, N=342)

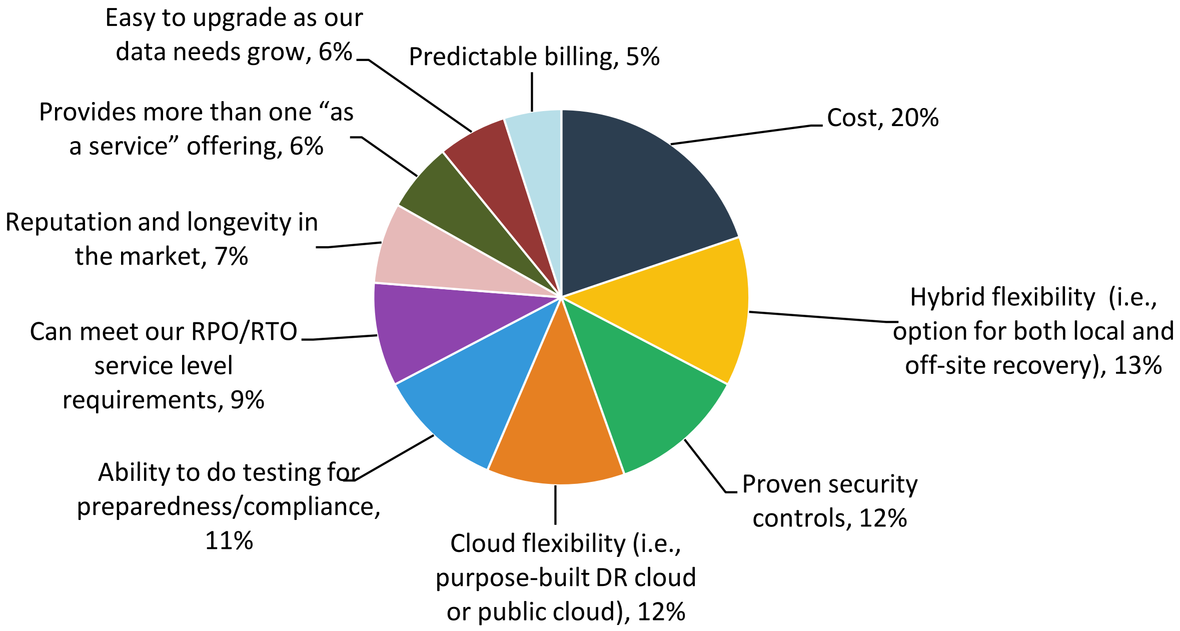


Source: Enterprise Strategy Group, 2016.

As a final consideration, Figure 27 shows the most important selection criteria for DRaaS providers in the eyes of potential adopters of these types of services, with cost, security, and multiple "flexibility" considerations topping the list.

Figure 27. Most Important Criteria for DRaaS Provider

If your organization were to utilize a DRaaS provider, what criteria would be most important? (Percent of respondents, N=142)



Source: Enterprise Strategy Group, 2016.

Conclusion

Organizations of all sizes are dependent on their data and IT services, though historically, only the largest of enterprises (or those in select markets) were able to justify the complexity and costs of legacy BC/DR remediation. Today, replication and failover technologies provide alternatives that are right-sized for any organization that needs better SLAs than what traditional backup/restore can provide, which means all of us.

For many, the primary obstacle to a redundant infrastructure is the secondary location, which is addressable by contemporary DRaaS offerings. Though arguably the most critical aspects of DRaaS-type offerings are not only the reliable secondary resources, but also the expertise in BC/DR planning and execution; skills which far surpass the abilities of many traditional backup administrators or IT operations personnel. That said, the mainstream approaches for BC/DR available in market today are opening the eyes of many who understood their IT dependencies, but presumed such IT agility was unattainable—and in the past, it was, but no longer.

Research Implications for Data Protection Vendors and Providers

When attempting to address IT organizations' BC/DR needs, data protection vendors and providers must:

- **Start by ensuring an understanding of the business needs, not the IT capabilities.** BC/DR is about ensuring the productivity and profitability of the business, by which the IT recovery features are a rather small (though critical) aspect. The choice of BC/DR technologies and IT approaches should be governed by the agility requirements of the business, not the other way around.
- **Contribute to the discussion through a broader range of stakeholders than the backup admin alone.** While many backup administrators might be the "front door" to the IT team, vendors and providers need to understand that most organizations have a much broader (and often more senior) group of folks who are planning and executing the BC/DR strategy and infrastructure.
- **Understand that BC/DR is more than "replication" or even IT.** While most recovery aspects of BC/DR are entirely dependent on the data as a starting point, BC/DR is much more about organizational process and culture. As such, do not over-sell your replication capability or failover function as "disaster recovery." Such technologies can *help* organizations achieve their BC/DR goals, but they are not in themselves "DR in a box."

Research Implications for IT and Data Protection Professionals

Start with understanding the needs of the business, include more individuals than you normally might in traditional data protection discussions, and then consider new approaches to achieving your goals. Remember:

- **BC/DR is driven by an assessment of the business impacts of outages of all sizes**, from server component failures to regional natural disasters. Each outage has a scale of impact, but each has a statistical likelihood to balance it out—e.g., a flood has far greater financial impact, but is relatively infrequent; whereas a server or host failure may only affect a few dozen VMs, but is almost inevitable. By assessing each for a business impact analysis (BIA), and through ongoing dialog with a broad range of IT and non-IT stakeholders, you will understand the scope of what your BC/DR plan should solve for and the financial boundaries to be managed.
- **Recovery isn't an "all or nothing" approach.** While you will likely only need to recover minority percentages of your environment at a time—from single servers/hosts through ROBOs to racks and server rooms—the unfortunate reality is that you don't know which percentages will require recovery, which necessitates the protection of the majority in order to recover the minority. This is not a bad thing. In fact, the more that your systems' level availability strategy is part of your organization-wide BC/DR strategy, the more ROI you'll be able to recognize by facilitating single-unit failovers for unplanned and planned outages.

Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of IT professionals from private- and public-sector organizations in North America (United States and Canada) between June 10, 2015 and June 26, 2015. To qualify for this survey, respondents were required to be IT professionals with day-to-day knowledge of and/or familiarity with their organization's data protection environment and strategy, specifically around technologies and processes to facilitate business continuity and disaster recovery. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 391 IT professionals.

Please see the *Respondent Demographics* section of this report for more information on these respondents.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

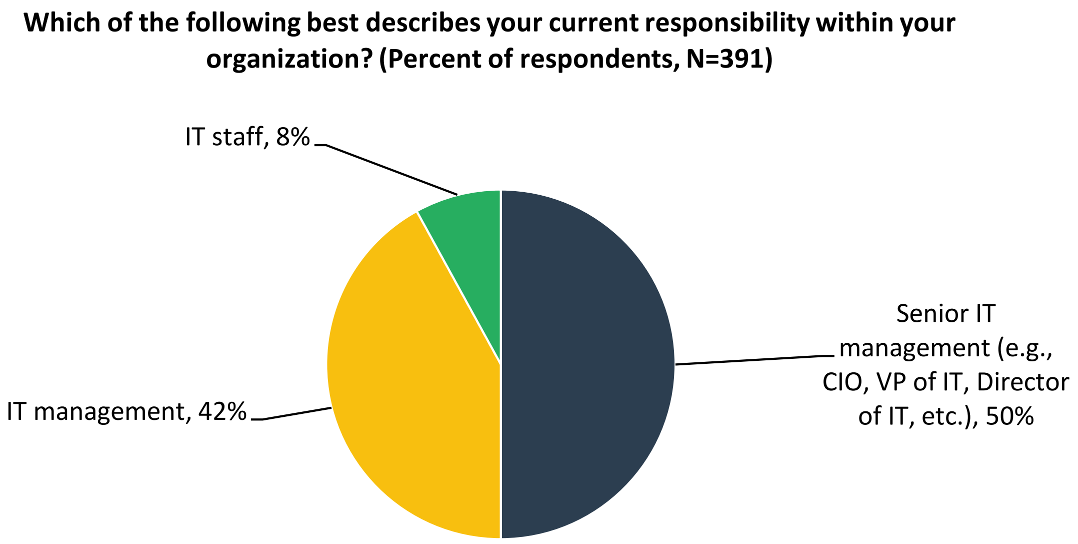
Respondent Demographics

The data presented in this report is based on a survey of 391 qualified respondents. The figures below detail the demographics of the respondent base, including individual respondents' current role, as well as respondent organizations' total number of employees, primary industry, and annual revenue, among others.

Respondents by Role

Respondents' current role within their organization is shown in Figure 28.

Figure 28. Survey Respondents by Current Role

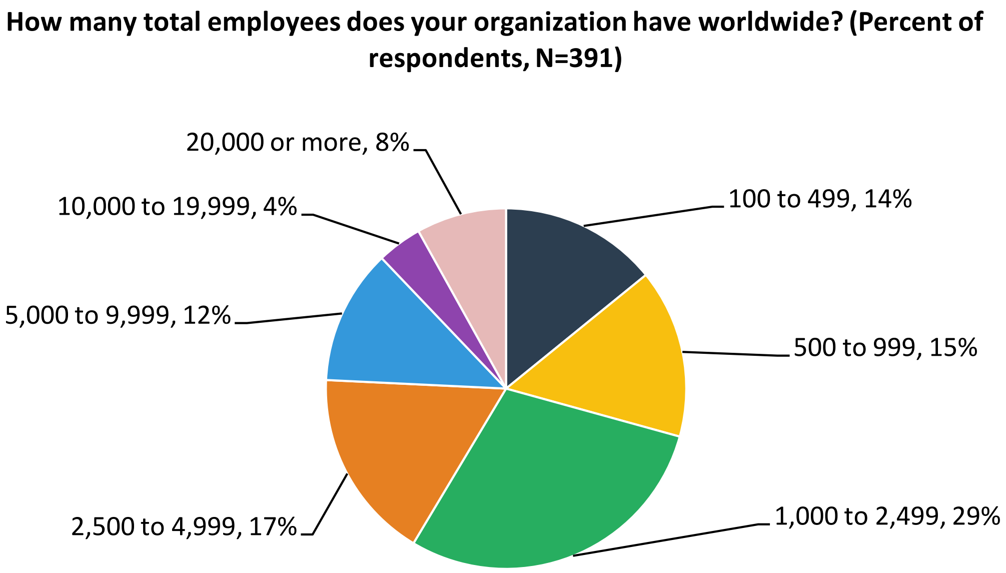


Source: Enterprise Strategy Group, 2016.

Respondents by Number of Employees

The number of employees in respondents' organizations is shown in Figure 29.

Figure 29. Survey Respondents by Number of Employees



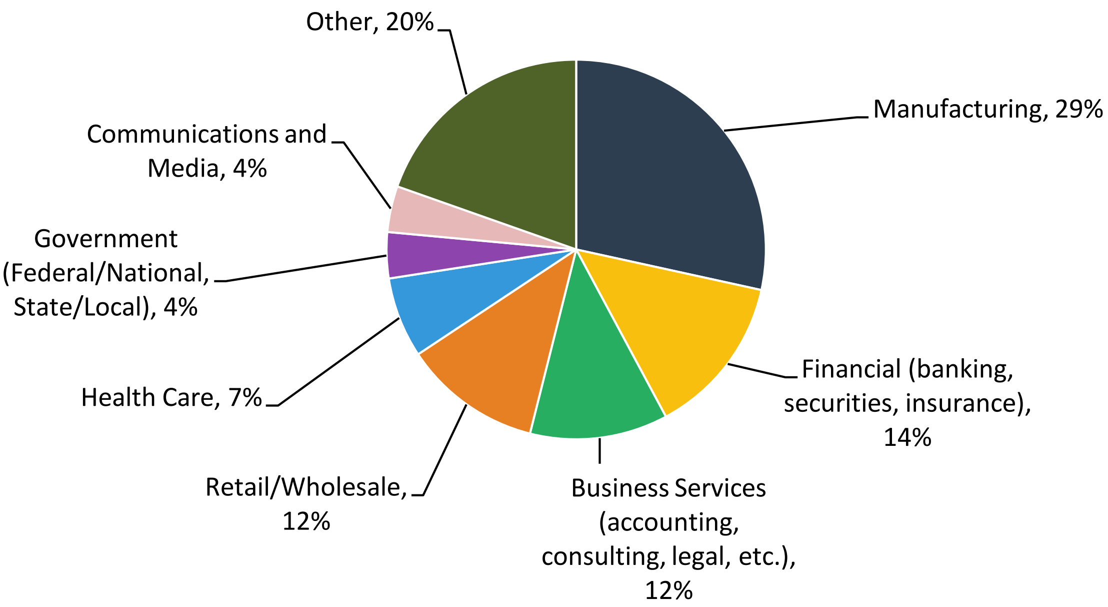
Source: Enterprise Strategy Group, 2016.

Respondents by Industry

Respondents were asked to identify their organization's primary industry. In total, ESG received completed, qualified responses from individuals in 19 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 30.

Figure 30. Survey Respondents by Industry

What is your organization's primary industry? (Percent of respondents, N=391)



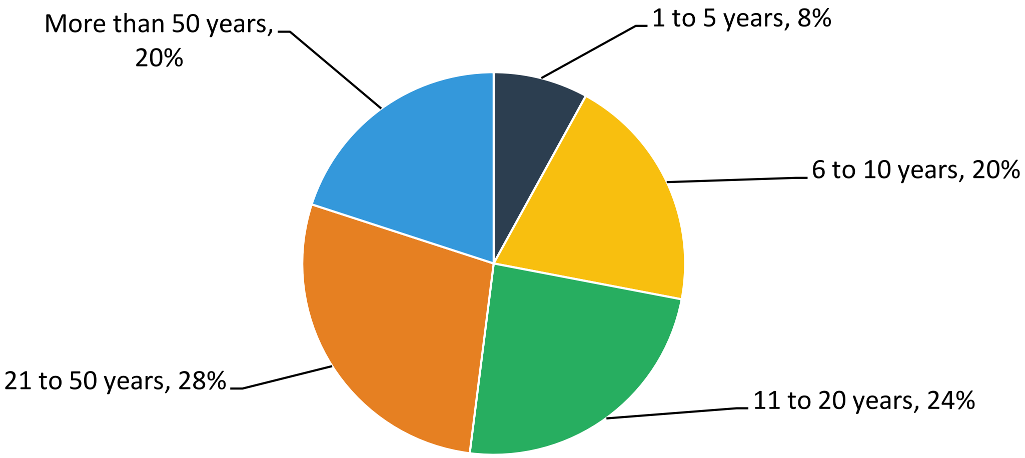
Source: Enterprise Strategy Group, 2016.

Respondents by Age of Organization

The age of respondents' organizations is shown in Figure 31.

Figure 31. Survey Respondents by Age of Organization

For approximately how long has your current employer been in existence? (Percent of respondents, N=391)

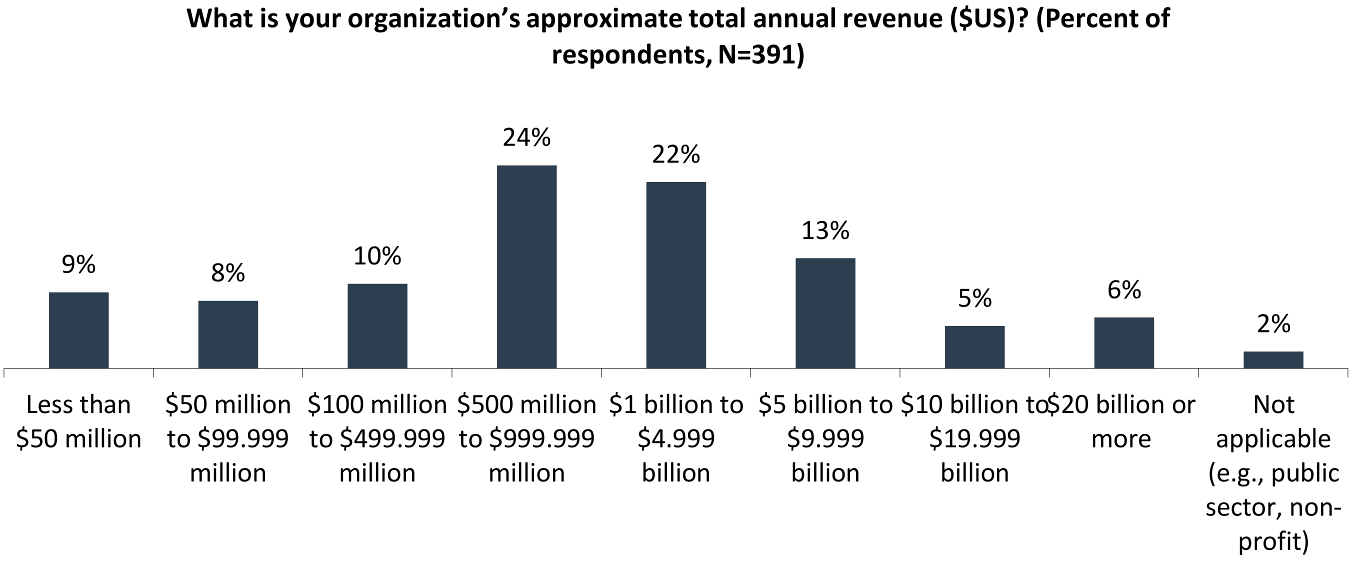


Source: Enterprise Strategy Group, 2016.

Respondents by Annual Revenue

Respondent organizations' annual revenue is shown in Figure 32.

Figure 32. Survey Respondents by Annual Revenue

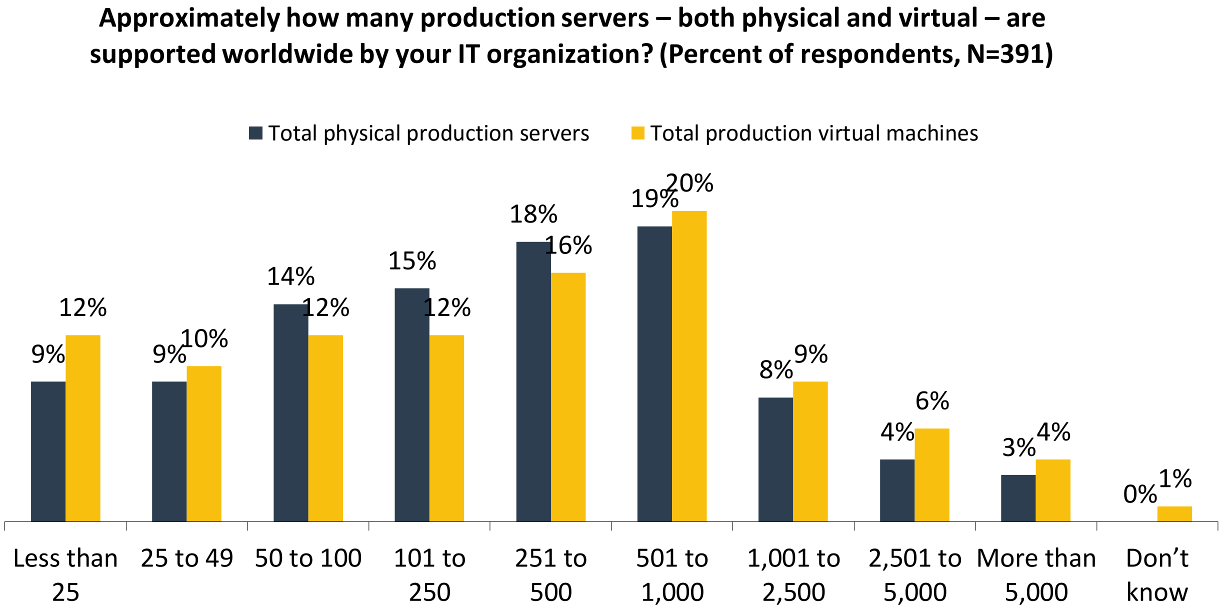


Source: Enterprise Strategy Group, 2016.

Respondents by Number of Production Servers

Respondent organizations' number of physical and virtual production servers is shown in Figure 33.

Figure 33. Survey Respondents by Total Number of Physical and Virtual Production Servers

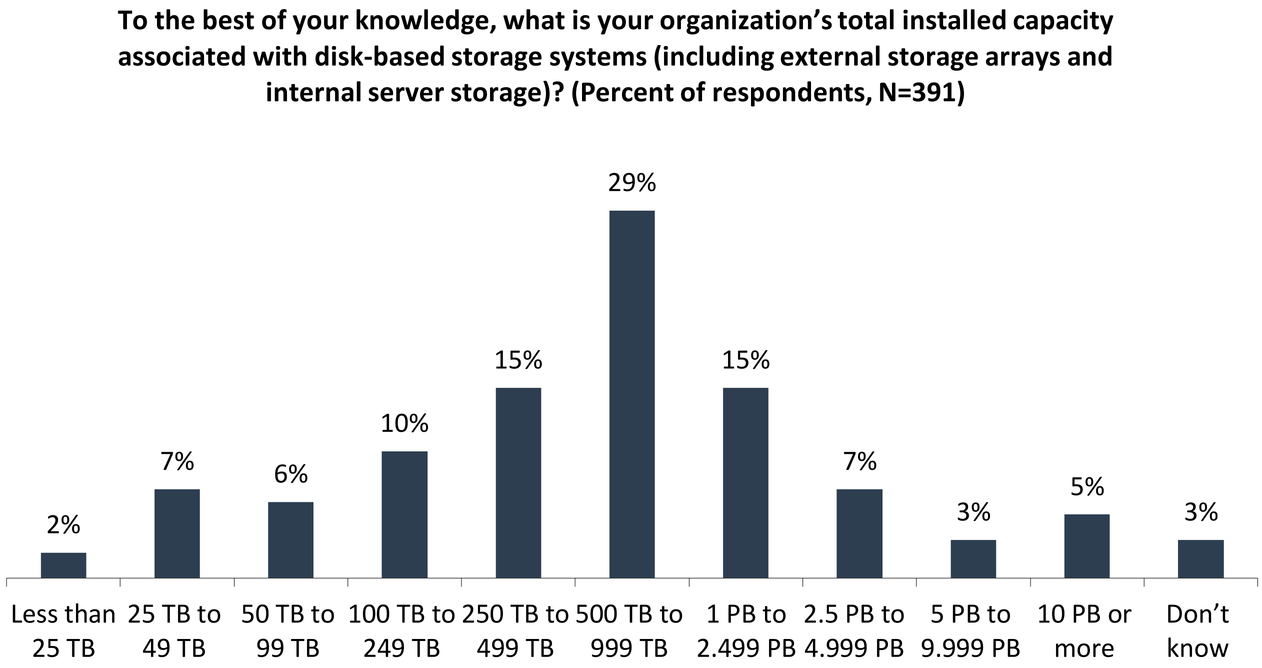


Source: Enterprise Strategy Group, 2016.

Respondents by Installed Disk-based Storage Capacity

Respondent organizations' total amount of disk-based storage capacity is shown in Figure 34.

Figure 34. Survey Respondents by Total Installed Disk-based Storage Capacity

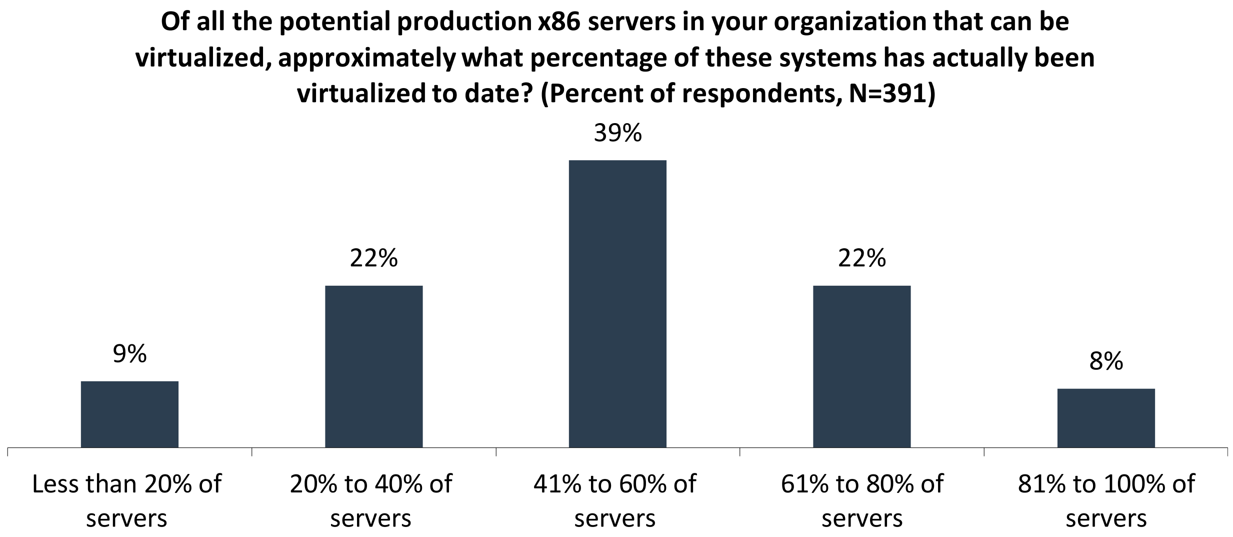


Source: Enterprise Strategy Group, 2016.

Respondents by Percentage of Virtualized x86 Servers

Respondent organizations' percentage of production x86 servers that have been virtualized to date is shown in Figure 35.

Figure 35. Survey Respondents by Percentage of Virtualized x86 Servers



Source: Enterprise Strategy Group, 2016.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0128 | www.esg-global.com