Research Report

Data Protection-as-a-service (DPaaS) Trends

By Jason Buffington, Senior Analyst and Bill Lundell, Senior Research Analyst

With Jennifer Gahm, Senior Project Manager and Adam DeMattia, Research Analyst

September 2013

Contents

List of Figures

List of Tables

Executive Summary

Report Conclusions

The "cloud" in all of its abstract and varied forms has created a wide range of new capabilities, misunderstandings, and potential pitfalls. While some see cloud-based delivery of traditional IT services as an enabler, others are left struggling to translate the hype into actionable solutions. All of these quandaries apply to the range of data protection solutions that are cloud-based. These data protection-as-a-service (DPaaS) offerings include:

> **Backup-as-a-service (BaaS)** – *Third-party service that includes software to back up data into a cloud-based repository, typically paid for using a capacity-protected model. Along with the software/service, it may also utilize an on-premises caching appliance or other onsite storage device for faster recovery, but the primary solution design is to ensure the data is stored via an Internet facility.*
>
> **Disaster recovery-as-a-service (DRaaS)** – *Third-party service that provides a means for whole servers, virtual machines, or applications (i.e., services) to be replicated to the cloud. In the event of a crisis, those servers or virtual machines can resume operation from the cloud provider, without having to first be restored to the on-premises data center. Backup of the individual files/data may not be included, but the primary function is the ability to resume services from the cloud.*
>
> **Storage-as-a-service (STaaS)** – *Third-party service that supplements a traditional backup solution—meaning a backup application that operates on-premises and makes copies of data to local/onsite media (such as tape, disk, etc.)—with a cloud-based storage service (i.e., capacity in the cloud) in order to have an offsite copy of the data that leverages cloud economics. This does not include cloud-based backup services with an on-premises caching appliance (i.e., this is not synonymous with BaaS).*

With these considerations in mind, ESG recently surveyed 306 IT professionals representing small (20 to 99 employees), midmarket (100 to 999 employees), and enterprise-class (1,000 employees or more) organizations in North America to determine current usage and interest levels in data protection-as-a-service (DPaaS) solutions, including backup-as-a-service (BaaS), disaster recovery-as-a-service (DRaaS), and cloud tertiary storage (STaaS). All respondents were responsible for data protection technology decisions for their organizations.

Based on the data collected from this survey in regard to DPaaS trends, ESG concludes:

- **Nearly one-quarter of organizations use cloud-based data protection services in some capacity.** Almost one-in-four respondent organizations is currently leveraging some type of cloud-based data protection service(s) to some extent, and another 46% have plans for or interest in doing so. Consistent with previous cloud computing data, larger organizations—as measured by typical annual data protection budgets—are more likely to be using or open to the possibility of using cloud-based data protection services.
- **Information security and budget constraints are the top impediments to the *initial* adoption and *more pervasive* usage of DPaaS.** The top concerns among both current cloud-based data protection users and those with no plans for or interest in these services were information security and budget constraints. Specifically, almost half of current users indicated that general data privacy concerns and/or the lack of appropriate security tools are impeding them from leveraging these services to an even greater extent. For their part, more than half of those organizations with no plans for or interest in cloud-based data protection services cited data security as an impediment to adoption in the form of privacy and/or the lack of appropriate tools.
- **Disaster recovery and cost-effectiveness are top DPaaS drivers.** In spite of the fact that cloud computing is presumed to have a superior cost model to traditional onsite IT deployments (data protection or otherwise), more than half of both current and potential users of DPaaS identified the ability to store data remotely for disaster recovery purposes as a reason for leveraging these services. However, the improved cost-effectiveness over traditional in-house solutions was also cited as a top reason for adopting DPaaS among both groups.

- **Cost reduction is the most commonly cited benefit among current DPaaS users.** More than two-thirds of current DPaaS users identify reduced costs as a usage benefit, whether in the form of infrastructure, personnel, power and cooling, support contracts, and/or software licensing. As far as other top benefits, more than one-third of current users report that cloud-based data protection services have fostered improved security. This is particularly interesting, considering that those organizations that are unsure of using cloud-based services more pervasively cite security as a primary concern.
- **Rogue cloud-based data protection services are becoming a real concern for IT.** Nearly half of IT respondents said they knew, or at least suspected, that employees in their organizations were using rogue DPaaS accounts. This is especially concerning because these services—whether DPaaS or online file sharing (OFS)—often enable employees to store corporate data and synchronize it across multiple devices, such as a home computer, tablet, or smartphone. Given the risk that personal accounts pose, it makes sense that more than half of organizations have a formal policy against end-users using personal DPaaS accounts to back up or store corporate data, although not all enforce these policies.
- **Cloud-based data protection services are most commonly procured from traditional backup software vendors and specialized service providers.** There are similar trends in terms of procurement sources for DRaaS and BaaS in that customers are recognizing that a key to their own success is partnering with providers that not only offer better economics and technical capabilities, but also possess experience in data protection services. In so doing, the service provider is more likely to keep the data protection software (including any agents at customer sites) running reliably, and remaining more agile and dependable for recoveries.
- **The majority of current BaaS users complement services with local (i.e., on-premises) resources.** Nearly one-quarter of current BaaS users report that their organizations have not yet had to go through a significant data recovery procedure, but only one-third of the organizations that have had to recover data from their BaaS providers claim that their recovery time objectives have always been achieved. In order to compensate for network shortcomings and/or difficulties (i.e., cost), many BaaS providers offer some type of workaround to help with bulk restores. When asked which approach is provided with their services, 41% of current BaaS users say an onsite caching appliance is included for faster restores. Nearly one-third report receiving either a hard drive with a copy of their data or an appliance that can be used to access data.
- **Current BaaS users would leverage services more pervasively if providers retained data longer.** Backup data in general is three times likelier than cloud-based backup data to be stored for at least six years, and not a single user of cloud-based backup services claims that her provider stores data for a period of more than ten years. However, nearly two-thirds of current BaaS users believe they would use cloud-based services to protect more applications/data if their provider offered longer-term retention.
- **Cloud-based disaster recovery services foster more frequent DR testing.** When asked about the frequency of disaster recovery testing from cloud-based secondary systems, 43% of current DRaaS users report doing so on a weekly or monthly basis. This is especially significant when compared to the frequency of testing within a self-hosted BC/DR plan—specifically, users of cloud-based DR services are more than three times as likely as those taking the do-it-yourself (DIY) approach to perform weekly recovery tests to determine whether and how quickly they could recover from a major outage.
- **Uncertainty persists about the compatibility of cloud capacity and on-premises backup applications.** One of the most disappointing revelations of the research was the fact that barely half of those respondents using cloud-based storage to store backup data believe that their on-premises backup solution is actually compatible with these services. If true, this speaks to the sluggish rate at which backup software vendors are evolving to take advantage of cloud storage. It is more likely, however, that IT respondents are unaware of whether or not their backup software is cloud-extensible.

Introduction

Research Objectives

In order to accurately assess organizations' current usage and interest in data protection-as-a-service (DPaaS) solutions—including backup-as-a-service (BaaS), disaster recovery-as-a-service (DRaaS), and cloud tertiary storage (STaaS)—ESG recently surveyed 306 IT professionals representing small (20 to 99 employees), midmarket (100 to 999 employees), and enterprise-class (1,000 employees or more) organizations in North America. All respondents were responsible for data protection technology decisions for their organizations.

The survey was designed to answer the following questions:

- Which methods of DPaaS are organizations currently using? Which methods of DPaaS are organizations planning to use in the next 12 months?
- Why are organizations using—or planning to use—cloud-based data protection services?
- Among organizations that *do not* use cloud-based data protection services, what are the leading adoption impediments? What—if anything—is preventing more pervasive usage among those organizations that already leverage these services?
- What benefits have organizations experienced as the result of using cloud-based data protection services?
- From which sources do organizations purchase—or expect to purchase—cloud-based data protection solutions?
- What is the current —or expected—scope of cloud-based data protection services in organizations?
- What is the approximate amount of data stored/expected to be stored in cloud-based data protection services?
- Which business applications are protected with cloud-based data protection services? Which business applications do organizations plan to protect with cloud-based data protection services?
- What amount of downtime can organizations tolerate with their cloud-based data protection services before experiencing significant revenue loss or other adverse business impact?
- What percent of applications are protected by cloud-based data protection services?
- What factors are preventing organizations from using cloud-based data protection services more pervasively?
- Are organizations using non-IT approved cloud-based data protection services?
- Do organizations have formal policies against individual employees and/or business groups using their own cloud-based data protection services?
- What actions do organizations take when employees are using an unsanctioned cloud-based data protection service?

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.

Research Findings

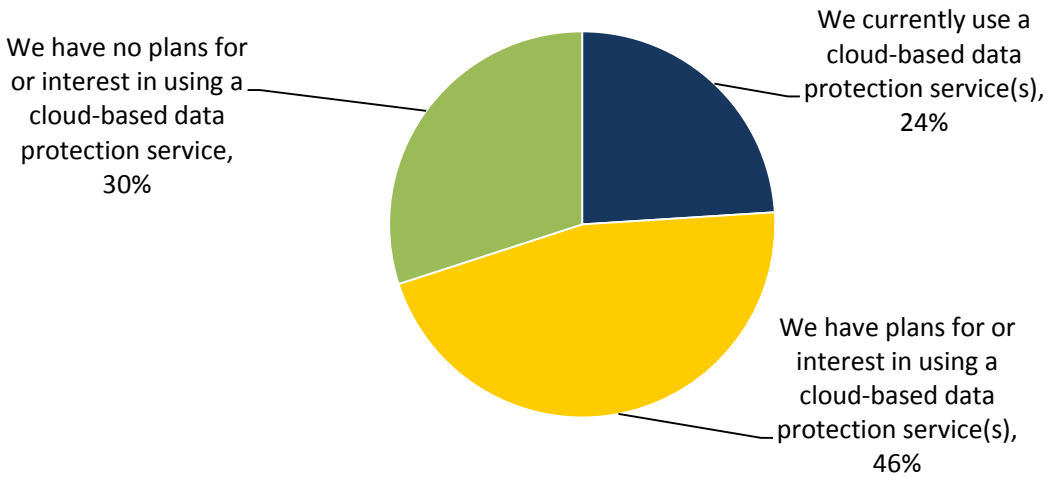
The State of the Cloud-based Data Protection Service Market

Data Protection-as-a-service (DPaaS) Adoption Drivers and Benefits Realized

As seen in ESG's *2013 Public Cloud Computing Trends* report, the use of cloud computing services is becoming an ever-more practical option for enterprise IT organizations. With this in mind, ESG surveyed IT professionals responsible for their organizations' data protection needs to gauge their willingness to consume that technology as a service. According to Figure 1, nearly one-quarter (24%) of respondent organizations are currently leveraging some type of cloud-based data protection service(s) in some capacity, and another 46% have plans for or interest in doing so. Consistent with previous cloud computing data, larger organizations—as measured by typical annual data protection budgets—are more likely to be using or open to the possibility of using cloud-based data protection services.

Figure 1. Usage Trends for Cloud-based Data Protection Services

What are your organization's plans for cloud-based data protection services (e.g., backup-as-a-service, disaster recovery-as-a-service, etc.)? (Percent of respondents, N=306)



Source: Enterprise Strategy Group, 2013.

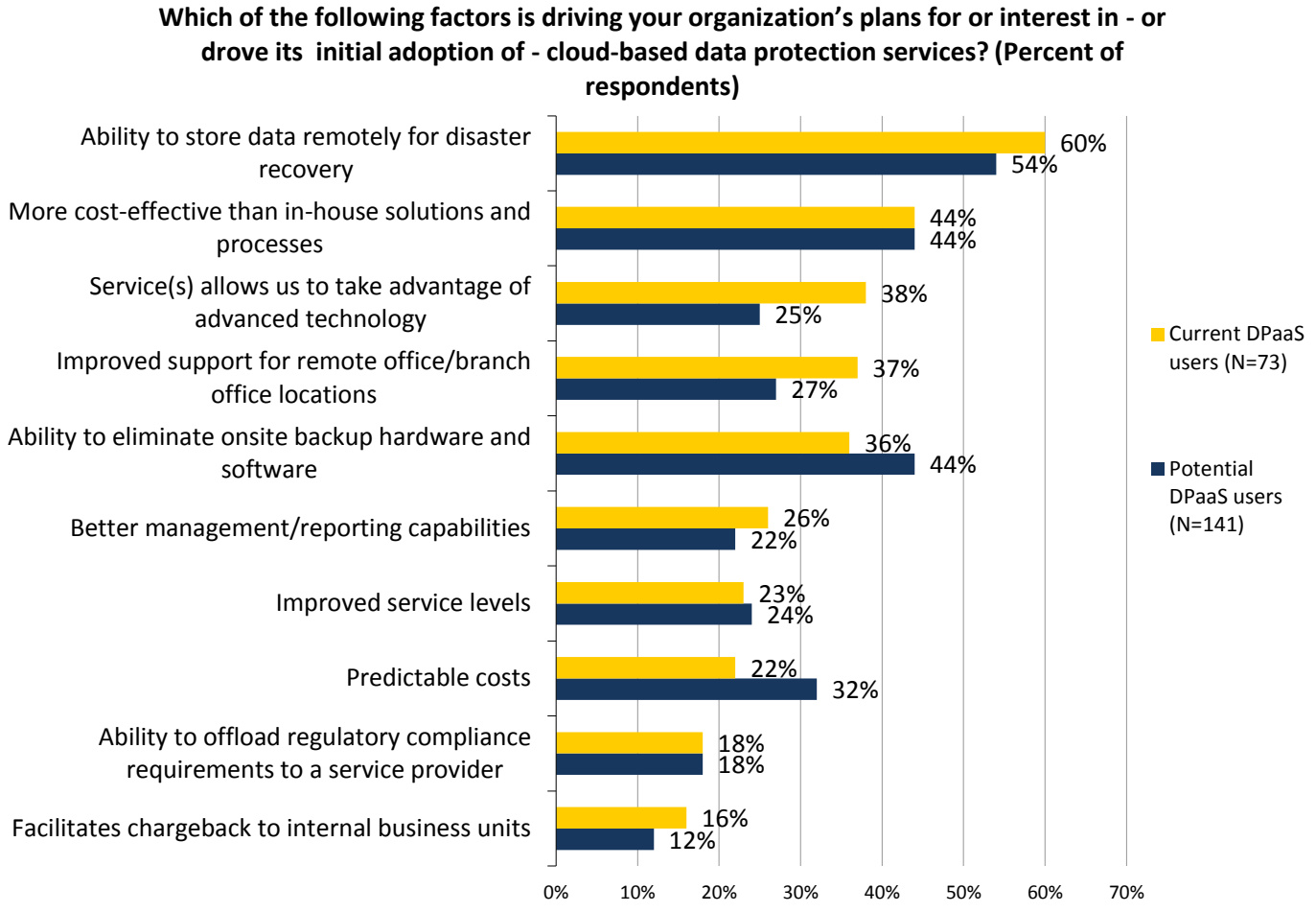
Table 1. Usage Trends for Cloud-based Data Protection Services, by Typical Annual Data Protection Budget

What are your organization's plans for cloud-based data protection services (e.g., backup-as-a-service, disaster recovery-as-a-service, etc.)?	By typical annual data protection budget		
	Less than $100,000 (N=81)	$100,000 to $999,999 (N=114)	$1m or more (N=83)
We currently use a cloud-based data protection service(s)	27%	19%	30%
We have plans for or interest in using a cloud-based data protection service(s)	35%	53%	49%
We have no plans for or interest in using a cloud-based data protection service(s)	38%	28%	20%
TOTAL	**100%**	**100%**	**100%**

Source: Enterprise Strategy Group, 2013.

In spite of the fact that cloud computing is presumed to have a superior cost model to traditional onsite IT deployments (data protection or otherwise), more than half of both current (60%) and potential (54%) users of DPaaS identified the ability to store data remotely for disaster recovery purposes as a reason for leveraging these services (see Figure 2). However, the improved cost-effectiveness over traditional in-house solutions was also cited as a top reason for adopting DPaaS among both groups. Cost is definitely a key consideration for potential users, which is reflected in the fact that eliminating onsite backup technologies—and undoubtedly their associated expenditures—and cost predictability were the other most common adoption drivers among potential users.

Figure 2. Adoption Drivers of Cloud-based Data Protection Services: Current vs. Potential Users



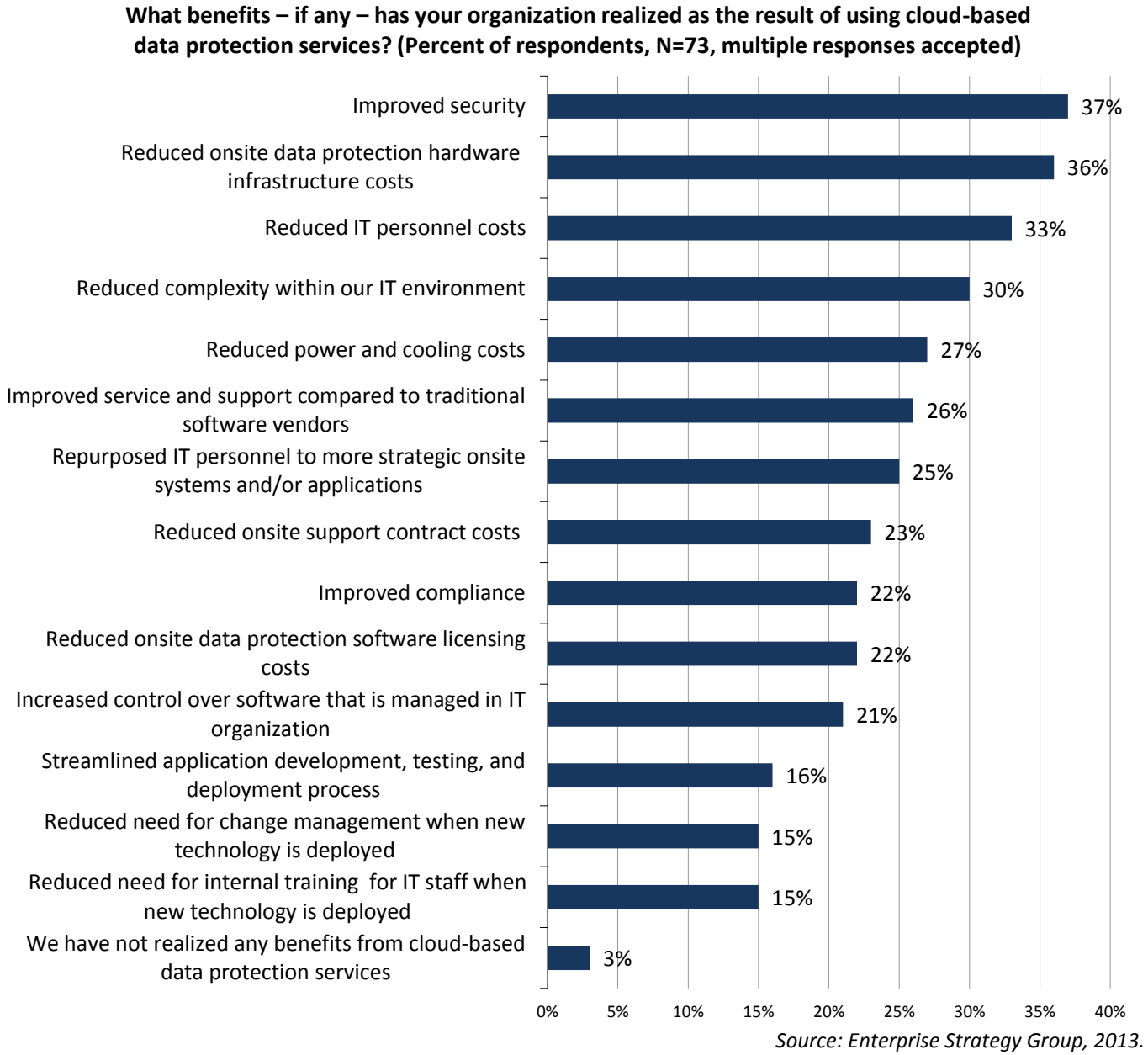
Source: Enterprise Strategy Group, 2013.

It is frequently hypothesized that organizations leverage cloud computing services as a way to save money, which is evident by virtue of the fact that 44% of current and potential users of cloud-based data protection services pointed to the cost-effectiveness of these solutions as an adoption driver. Figure 3 appears to validate that theory, with more than two-thirds (71%) of current DPaaS users identifying reduced costs as a usage benefit, whether in the form of infrastructure (36%), personnel (33%), power and cooling (27%), support contracts (23%), and/or software licensing (22%).

As far as other top benefits, more than one-third (37%) of current users report that cloud-based data protection services have fostered improved security. This is particularly interesting, considering that those organizations that are unsure of using cloud-based services more pervasively cite security as a primary concern. But from a practical perspective, many environments may find that data tapes (and the potential to accidentally or intentionally lose them) and the ease with which disk-based copies can be created are more precarious from a security perspective than a cloud-based service.

From an IT headcount perspective, in addition to staffing-related costs, DPaaS has enabled organizations to repurpose personnel to protect more strategic onsite systems/applications (25%) and/or reduce the need for IT staff training (15%). It is worth noting that only 3% of current cloud users claim to have realized no benefits from leveraging cloud services.

Figure 3. Benefits Derived from the Usage of Cloud-based Data Protection Services



Source: Enterprise Strategy Group, 2013.

Factors Preventing Initial Adoption or More Pervasive Usage of Cloud-based Data Protection Services

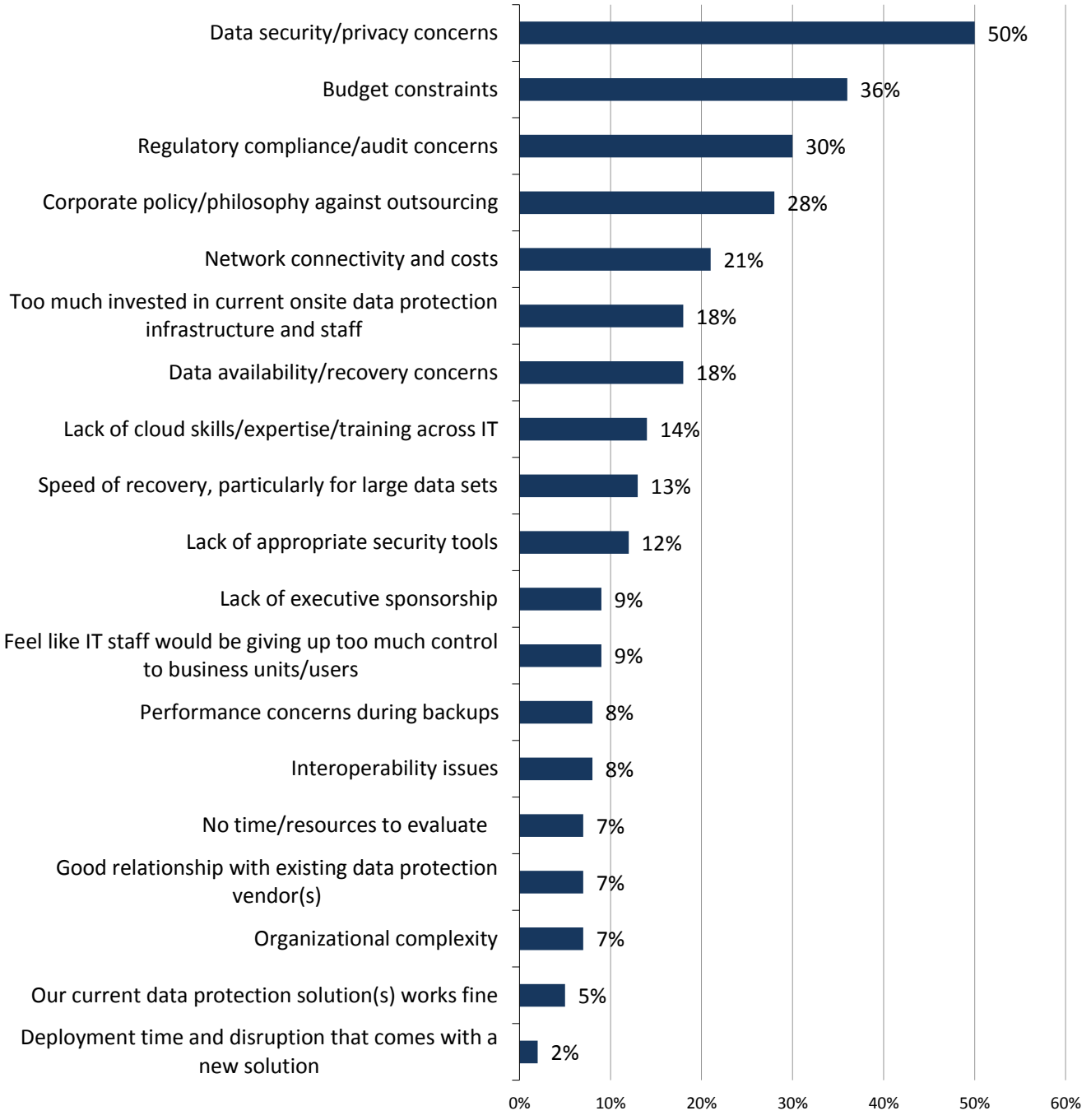
Those organizations that do not currently use cloud-based data protection services and have no plans to do so were asked to identify the factors holding them back from adoption. Not surprisingly, Figure 4 reveals that more than half (52%) of these respondents cited data security as an impediment in the form of privacy (50%) and/or the lack of tools (12%), which is consistent with previously conducted ESG research on the topic of cloud computing.[1] Other top objections among non-adopters included budget constraints (36%), regulatory compliance concerns (30%), and

[1] Source: ESG Research Report, *2013 Public Cloud Computing Trends*, March 2013.

a corporate philosophy against outsourcing (28%). The most commonly identified *technology-specific* inhibitor (i.e., non-business policy or mandate) was the expected network connectivity and cost implications of DPaaS.

Figure 4. Factors Preventing Initial Adoption of Cloud-based Data Protection Services

In general, which of the following factors would you say are preventing your organization from using cloud-based data protection services? (Percent of respondents, N=92, multiple responses accepted)

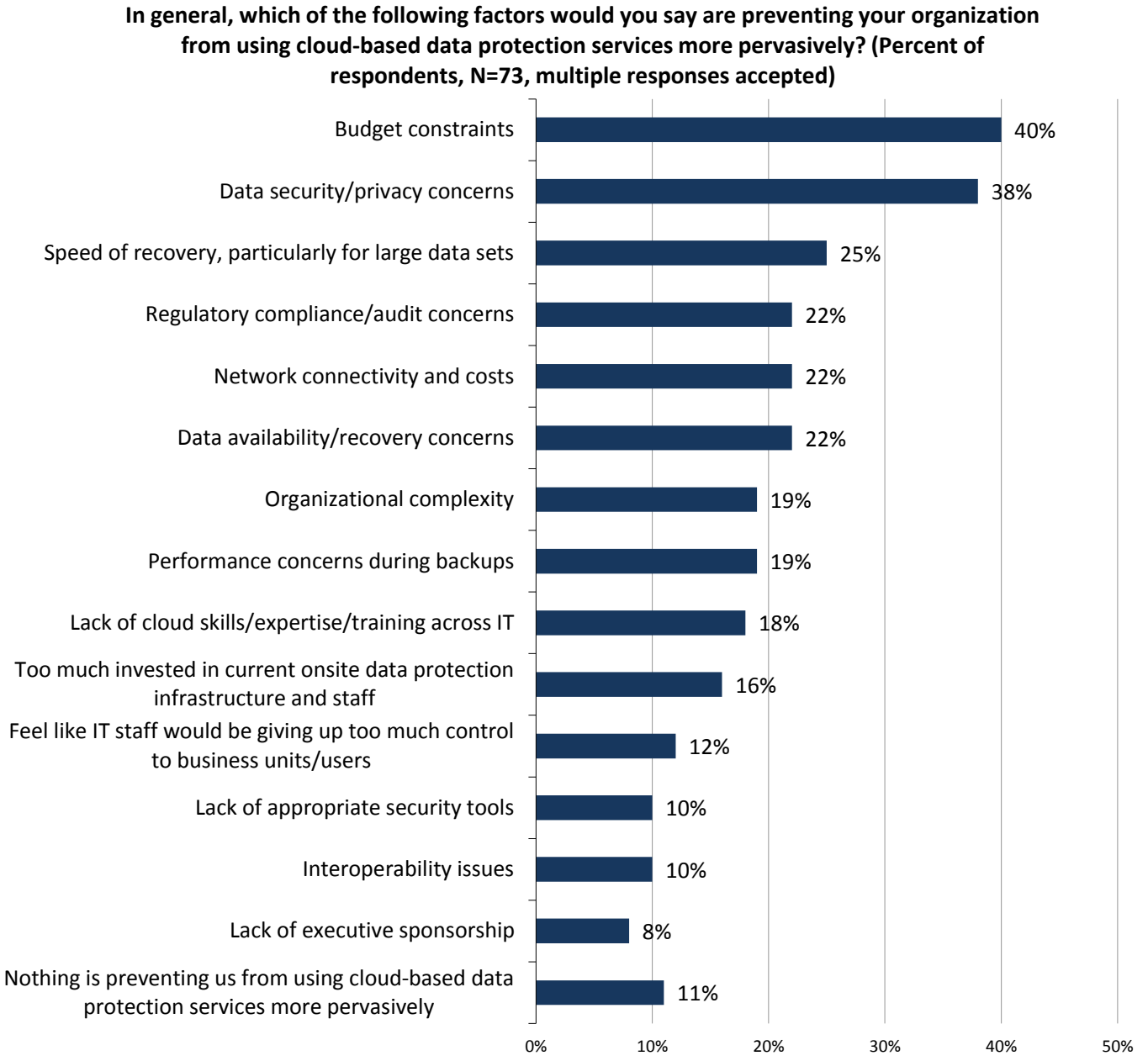


Source: Enterprise Strategy Group, 2013.

Like their DPaaS-averse counterparts, the most common factors preventing more pervasive usage of these services among current users are budget constraints and security concerns (see Figure 5). Specifically, almost half (45%) of these organizations indicated that general data privacy concerns (40%) and/or the lack of appropriate security tools (10%) are impeding them from leveraging these services to an even greater extent. It also warrants mentioning that

one-quarter of current users have experienced performance issues when it comes to data recovery, especially for large data sets.

Figure 5. Factors Preventing More Pervasive Usage of Cloud-based Data Protection Services



Source: Enterprise Strategy Group, 2013.

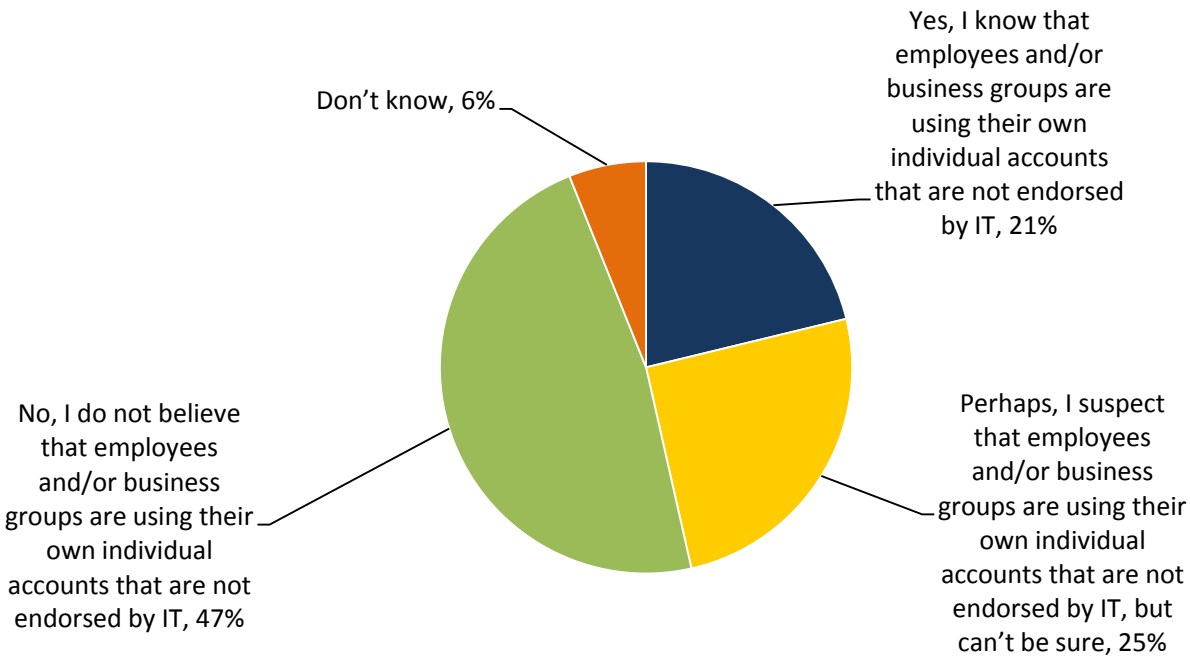
Rogue DPaaS Usage

As a result of the bring-your-own-device (BYOD) and consumerization of IT movements, individual employees are increasingly signing up for free consumer-based cloud services to back up and/or store their data, often without any permission from or knowledge of their employer. ESG calls these "rogue" accounts because IT teams have no control over how the personal accounts are used, and sometimes may not even know that the accounts exist. Rogue accounts pose a risk to organizations because corporate data and intellectual property may be stored in them, yet IT has no way of applying the organization's security and access policies to the accounts in order to protect those assets.

When asked about the usage of non-IT approved cloud-based data protection services, nearly half (46%) of respondents said they knew (21%), or at least suspected (25%), that employees in their organizations were using rogue DPaaS accounts (see Figure 6). This is especially concerning because these services—whether DPaaS or online file sharing (OFS)—often enable employees to store corporate data and synchronize it across multiple devices, such as a home computer, tablet, or smartphone. Consequently, if an employee with a personal DPaaS account leaves his employer, he still owns the account and any corporate data stored therein still resides in that account and is accessible by the (now former) employee through his personal devices. Clearly, this can create an unacceptable security, legal, and business risk for employers.

Figure 6. Employee Usage of Non-IT-approved Cloud-based Data Protection Services

Do you know if employees and/or business groups in your organization are using non-IT approved cloud-based data protection services (i.e., they are using their own individual accounts)? (Percent of respondents, N=306)



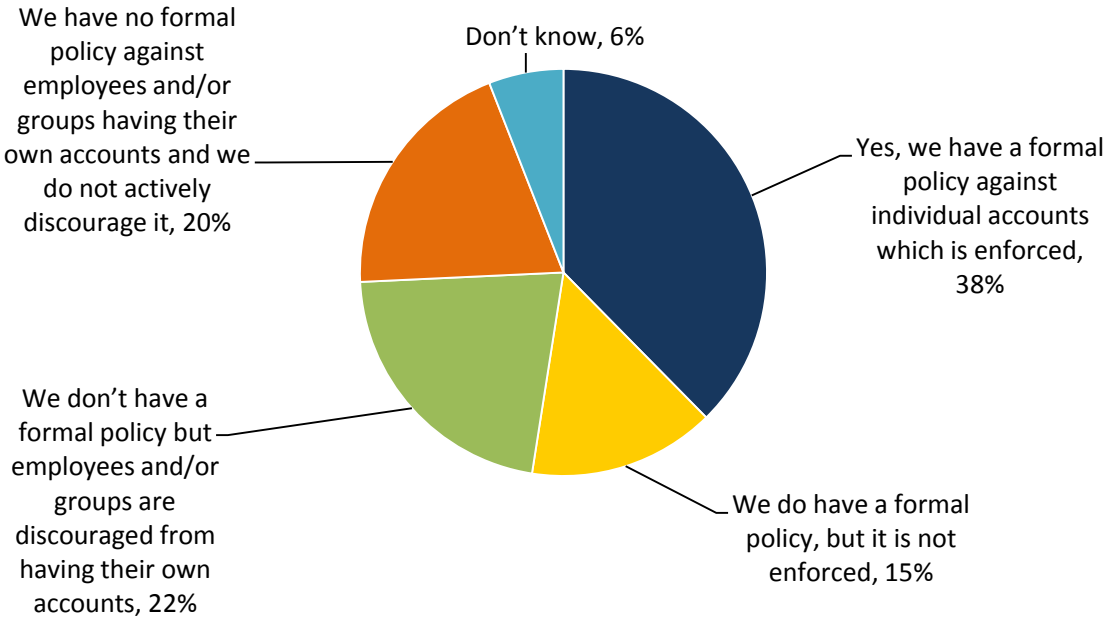
Source: Enterprise Strategy Group, 2013.

Given the risk that personal accounts pose, it makes sense that more than half (53%) of organizations have a formal policy against end-users using personal DPaaS accounts to back up or store corporate data, although not all enforce these policies (see Figure 7). The remaining organizations have not created a policy and only about half of that group has even discouraged employees from using individual accounts.

Upon discovering a rogue account, more than half (58%) of the organizations that have formal policies against rogue DPaaS accounts—or at least discourage their use—indicate that they move quickly to shut down the unauthorized services (see Figure 8). ESG has heard anecdotal evidence of some companies upholding policies against users having personal accounts that go as far as terminating employees found to be in violation of the policy. Nearly one-quarter (23%) of these organizations do not take any action when they discover rogue accounts other than simply keeping a record of the account(s), which they may act upon later, while 13% are doing absolutely nothing because—despite having a formal policy against unauthorized DPaaS accounts in place in some cases—they do not yet have a process in place for *handling* rogue accounts.

Figure 7. Policies Against Employee Usage of Non-IT-approved Cloud-based Data Protection Services

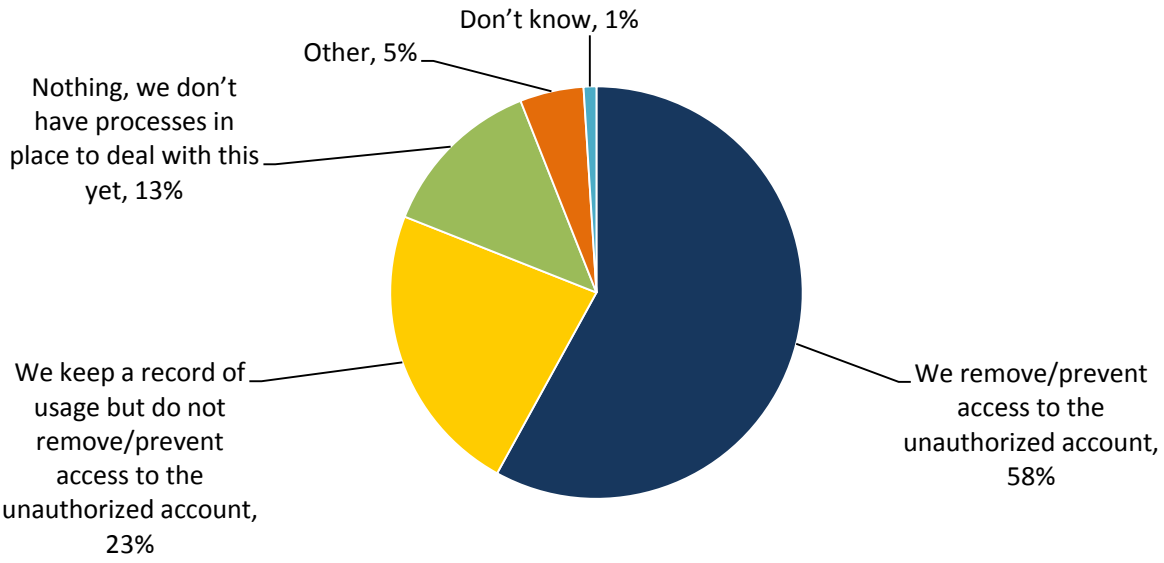
Does your organization have a formal policy against individual employees and/or business groups using their own cloud-based data protection service accounts? (Percent of respondents, N=306)



Source: Enterprise Strategy Group, 2013.

Figure 8. Actions Taken Against Employees Using Unsanctioned Cloud-based Data Protection Services

Generally speaking, what course of action does your organization take if/when it discovers an individual employee and/or business group is using an unsanctioned cloud-based data protection service? (Percent of respondents, N=228)



Source: Enterprise Strategy Group, 2013.

Backup-as-a-service (BaaS) Usage Trends

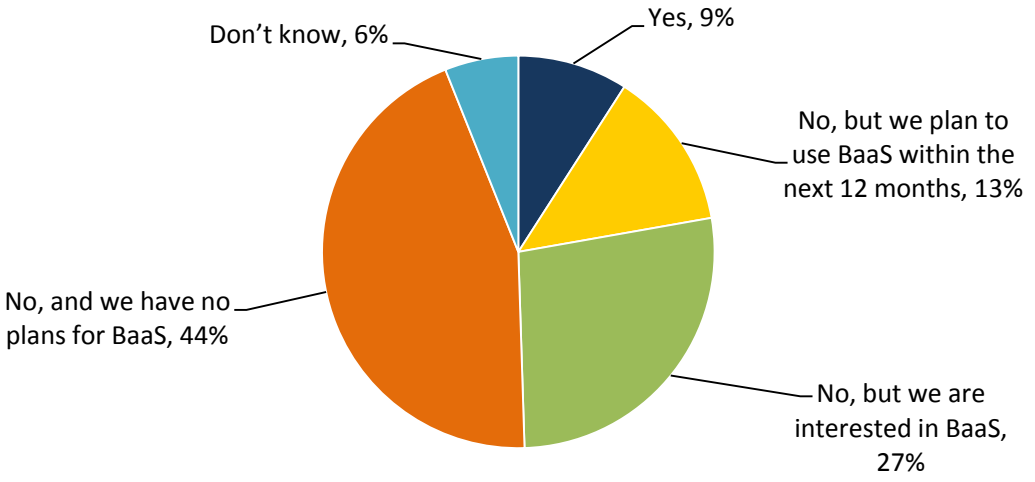
In order to gauge adoption levels for cloud-based backup services, ESG asked respondents if any of their applications and/or systems were backed up via the BaaS model. For the purposes of this report, backup-as-a-service was defined as follows:

> *Third-party service that includes software to back up data into a cloud-based repository, typically paid for using a capacity-protected model. Along with the software/service, it may also utilize an on-premises caching appliance or other onsite storage device for faster recovery, but the primary solution design is to ensure the data is stored via an Internet facility.*

According to Figure 9, only 9% of survey respondents currently use BaaS to protect data, while an additional 40% have plans for or interest in these cloud-based backup services. As was the case with DPaaS in general, organizations with larger data protection budgets are most likely to be currently using or open to the possibility of using BaaS (see Table 2).

Figure 9. Usage Trends for Backup-as-a-service (BaaS)

Is your organization currently using backup-as-a-service (BaaS) to protect any of the data associated with its applications and/or systems (including employee endpoint devices like desktop/laptop PCs and mobile devices)? (Percent of respondents, N=306)



Source: Enterprise Strategy Group, 2013.

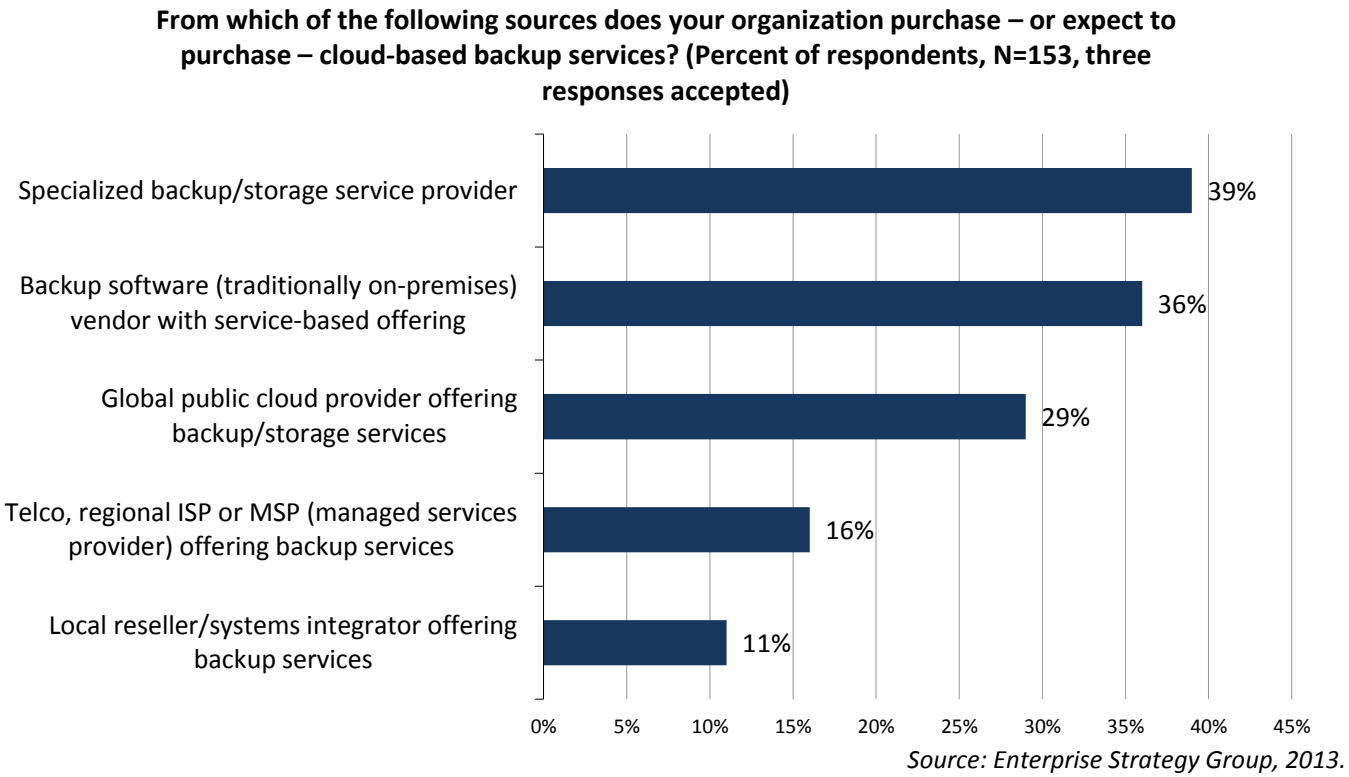
Table 2. Usage Trends for Backup-as-a-service (BaaS), by Typical Annual Data Protection Budget

Is your organization currently using BaaS to protect any of the data associated with its applications and/or systems (including employee endpoint devices like desktop/laptop PCs and mobile devices)?	By typical annual data protection budget		
	Less than $100,000 (N=77)	$100,000 to $999,999 (N=110)	$1m or more (N=80)
Yes	12%	9%	13%
No, but we plan to use BaaS within the next 12 months	5%	15%	25%
No, but we are interested in BaaS	23%	30%	35%
No, and we have no plans for BaaS	60%	46%	28%
TOTAL	**100%**	**100%**	**100%**

Source: Enterprise Strategy Group, 2013.

Current and potential BaaS users were then asked to identify the source(s) from which they purchase—or expect to purchase—cloud-based backup services. As seen in Figure 10, more than one-third of these organizations procure these services from specialized backup/storage service providers (39%) and/or traditional backup software vendors (36%). At the other end of the spectrum, current and potential BaaS users were significantly less likely to procure cloud-based backup services from either telcos and regional ISPs or local VARS and SIs.

Figure 10. Source(s) from Which Current & Potential BaaS Users Expect to Purchase Cloud-based Backup Services



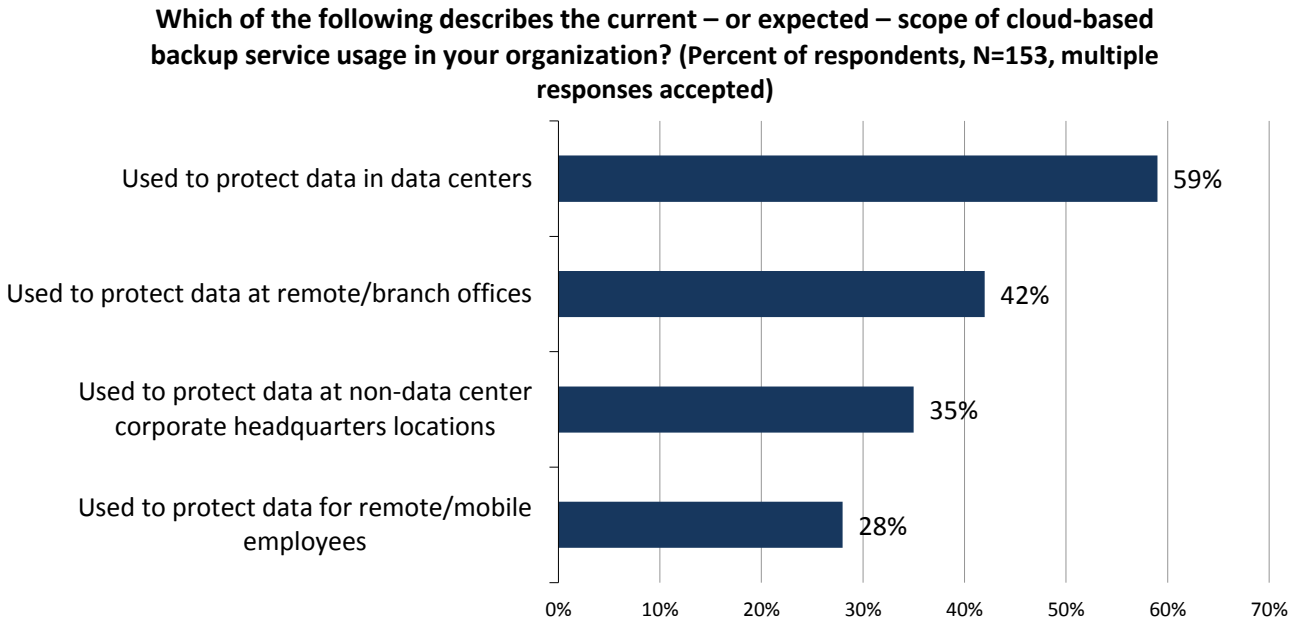
Source: Enterprise Strategy Group, 2013.

Figure 10's findings are reasonable considering that, as cloud-services become more commonplace and more clearly understood as simply a method of delivery, IT decision makers would likely be most interested in consuming the "capability" of BaaS from either a specialty backup-service provider or a backup software vendor, since they focus on backup, in contrast to a public cloud provider, telco/ISP, or reseller—none of which technically have deeper backup expertise than the IT organizations themselves.

A majority of current and potential BaaS users protect—or expect to protect—data running on data center-resident systems (see Figure 11). Cloud-based backup services protecting data at remote/branch office locations is the next most commonly cited use case, which is not surprising given that this is an established IT challenge from both a ROBO and a data protection perspective.[2] [3] This also makes sense given that many IT organizations presume that their intranet-connected data center is actually the remote location for branch office and endpoint data, thus not presuming to send their edge-based data to a BaaS provider, whereas data centers need a secondary location to back up to—which might be either a self-managed site (with the OPEX and CAPEX that go with it) or a BaaS provider—as Figure 11 shows.

[2] Source: ESG Research Report, *Remote Office/Branch Office Technology Trends*, July 2011.
[3] Source: ESG Research Report, *Trends in Data Protection Modernization*, August 2012.

Figure 11. Current or Expected Scope of Cloud-based Backup Service Usage



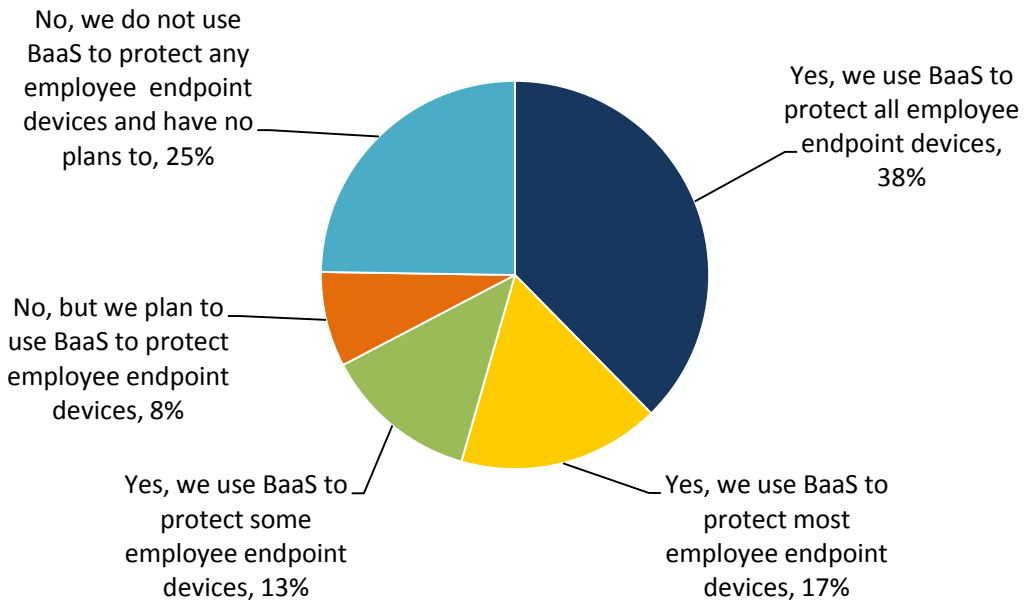
Source: Enterprise Strategy Group, 2013.

Previously conducted ESG research revealed that a majority of organizations had no formal policies in place to back up endpoint devices like desktop and laptop PCs or even smartphones.[4] Along with other considerations, that disparity leads to the common hypothesis that the protection of endpoint devices is a use case for cloud-based backup services. As such, it is not surprising to see that more than two-thirds (68%) of current BaaS users protect their employees' endpoint devices, and another 8% plan to do so going forward (see Figure 12).

[4] Source: ESG Research Report, *Endpoint Device Backup Trends*, December 2010.

Figure 12. Protecting Endpoint Devices with Cloud-based Backup Services

Does your organization back up the endpoint devices that its employees use to do their jobs via BaaS? (Percent of respondents, N=24)

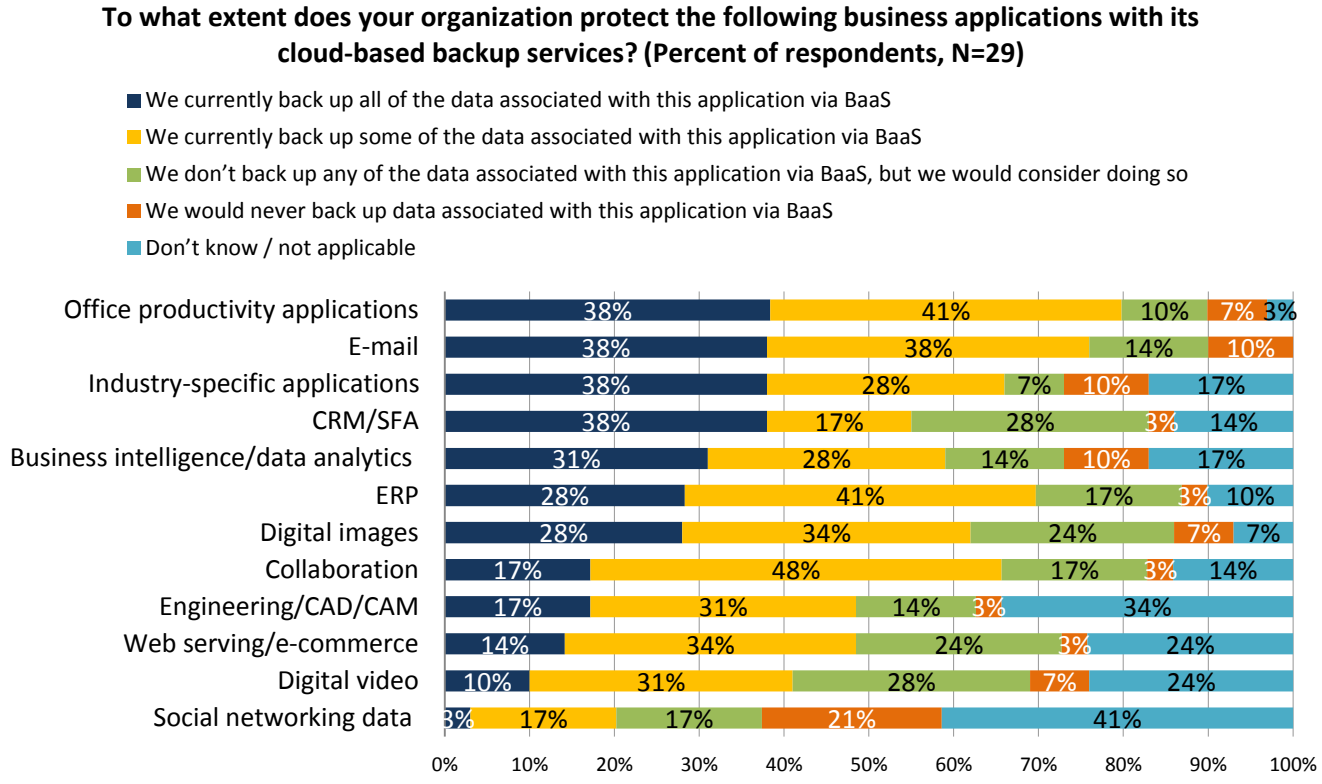


Source: Enterprise Strategy Group, 2013.

Which specific applications are current users protecting via the BaaS model? As shown in Figure 13, more than one-third (38%) of current users leverage BaaS to protect *all* of the data associated with office productivity applications, e-mail, customer relationship management (CRM) software, and industry-specific applications. In addition to these relatively mature categories, more than half of current BaaS users protect all or some of the data associated with their BI/analytics platforms. Prior ESG research has shown that not only has data protection become a key priority as analytics platforms get used for more real-time activities, but also that there is a lack of backup knowledge and skills in this area.[5] As such, it makes sense that organizations would look to circumvent these issues by offloading data protection responsibilities to a third-party. The other applications most commonly protected either exclusively or at least in part by cloud-based backup services include ERP (69%) and collaboration (65%) software.

In considering Figure 13, the bottom of the list is equally reasonable. Social networking data is almost all cloud-based already and thus presumed to not require additional backups, while web serving and e-commerce platforms are typically just the front-end interfaces, which would be protected locally.

Figure 13. Applications Current BaaS Users Protect with Cloud-based Backup Services

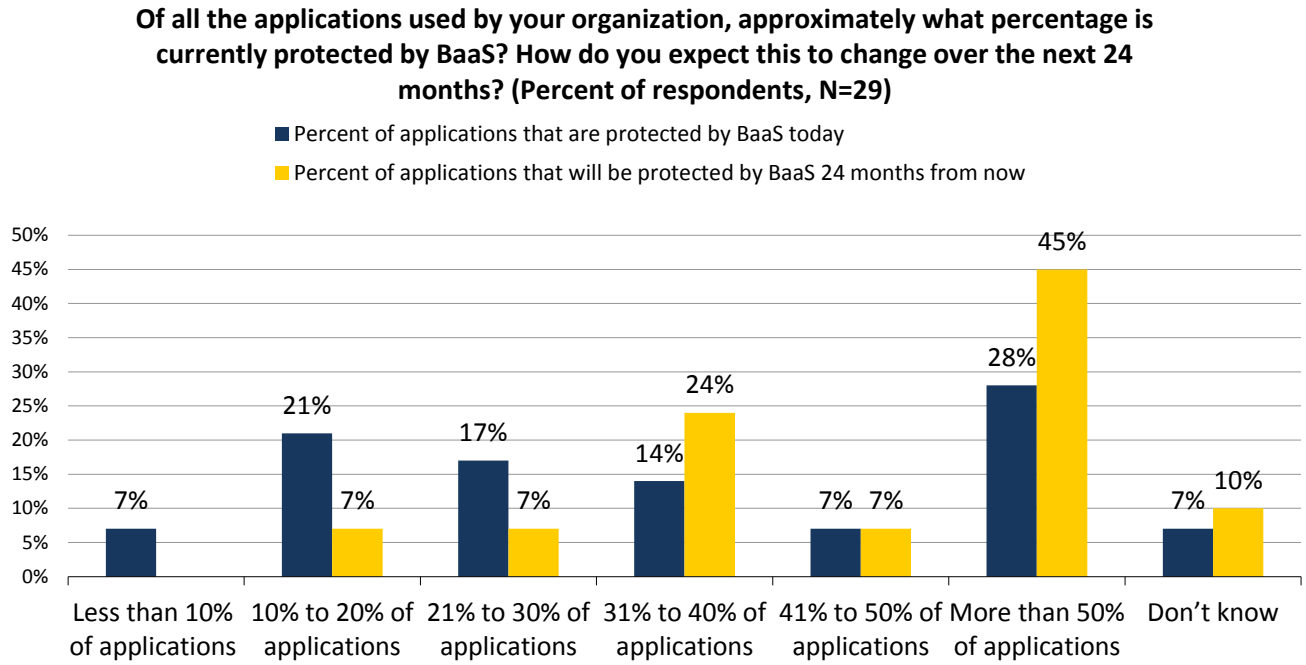


Source: Enterprise Strategy Group, 2013.

When analyzing current BaaS usage trends, in addition to the types of applications being protected with cloud-based backup services, it is important to establish the extent to which applications are being protected via the online service model relative to an organization's entire application footprint. In order to answer this question, current BaaS users were asked to consider all of the business applications used by their organizations and then determine the percentage of these applications protected with cloud-based backup services today as well as how they expect this to change over the next two years. While the current scope of BaaS usage is relatively limited within most organizations, a significant shift is expected to occur over the next 24 months. Specifically, while 59% of organizations protect no more than 40% of their applications via BaaS today, more than half (52%) believe that cloud-based backup services will be responsible for safeguarding the data associated with in excess of 40% of their applications by 2015 (see Figure 14).

[5] Source: ESG Research Report, *The Convergence of Big Data Processing and Integrated Infrastructure*, July 2012.

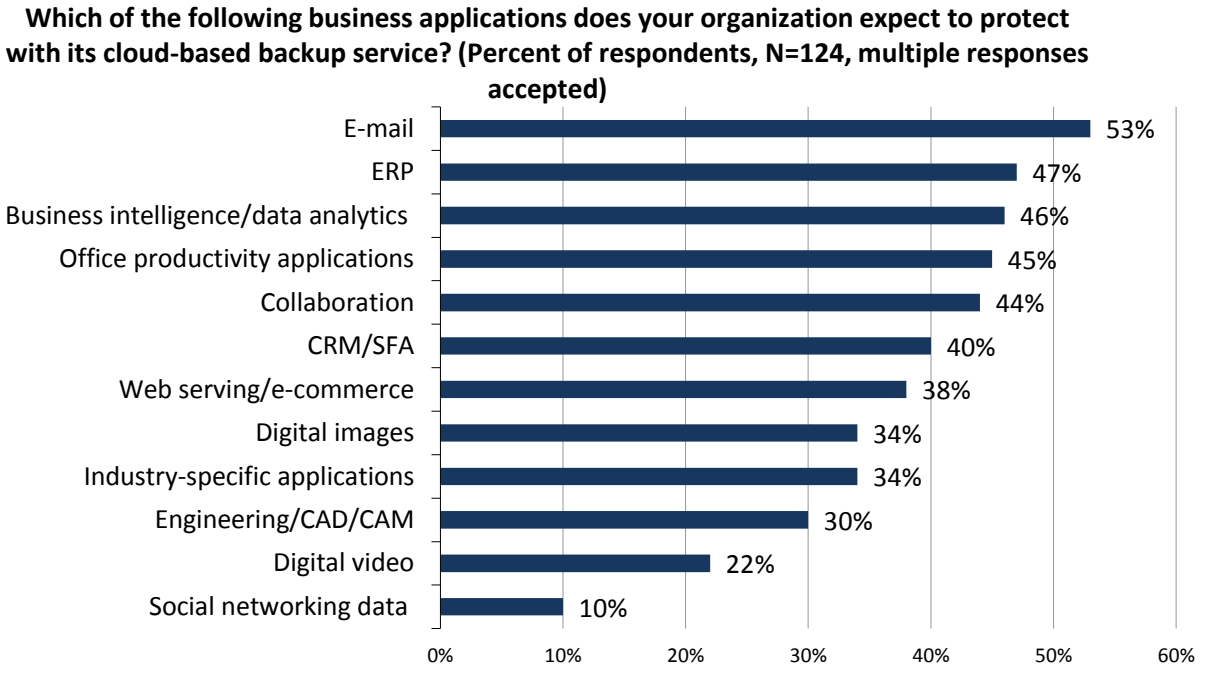
Figure 14. Extent of BaaS Usage, Now and 36 Months from Now



Source: Enterprise Strategy Group, 2013.

Potential BaaS users follow a fairly similar adoption pattern as those organizations already using cloud-based backup services. Specifically, more than half (53%) of these respondent organizations plan to protect e-mail with BaaS, while 47% expect to back up their ERP data to the cloud (see Figure 15).

Figure 15. Applications Potential BaaS Users Expect to Protect with Cloud-based Backup Services

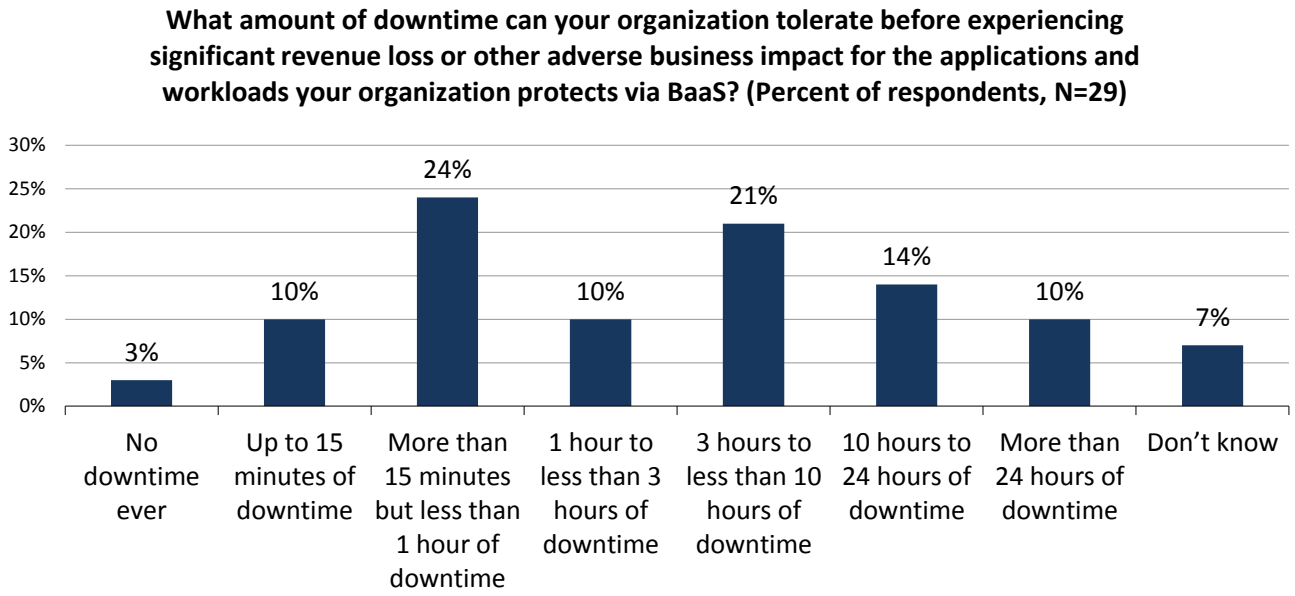


Source: Enterprise Strategy Group, 2013.

It is clear that a number of organizations currently protect an assortment of business- and even mission-critical applications/workloads with cloud-based services. Since lack of application availability or loss of vital information can result in missed business opportunities, reduced productivity, lost revenue, dissatisfied customers, damage to

the company's reputation, and even legal liability, it follows that more than one-third (37%) of current BaaS users indicated that downtime for those applications protected by cloud-based services cannot exceed more than an hour without causing adverse business impact (see Figure 16).

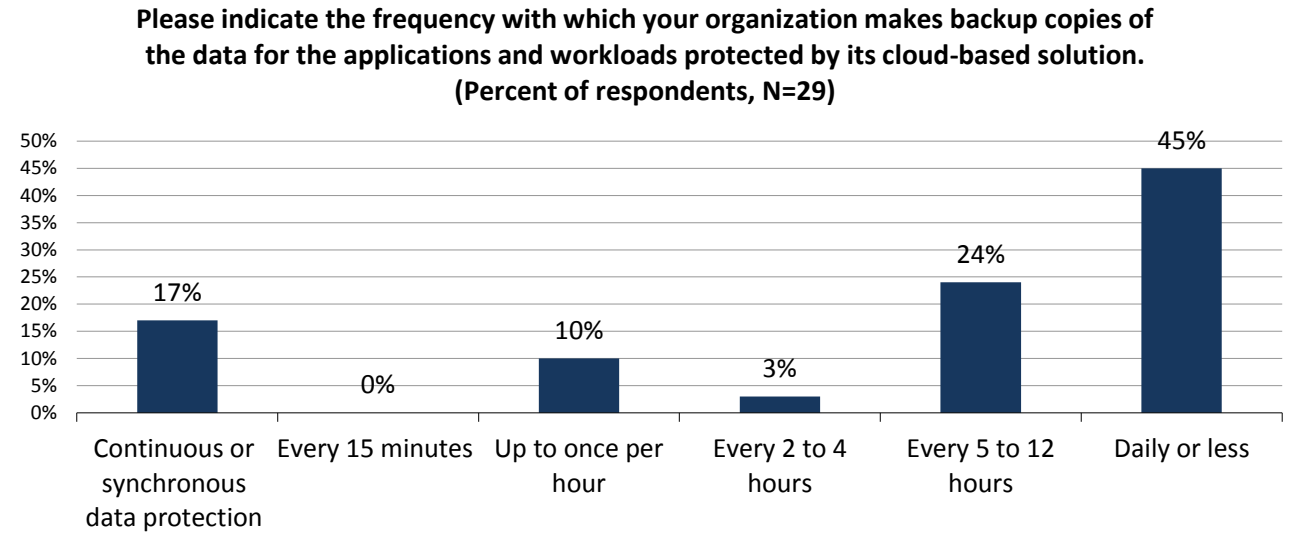
Figure 16. Downtime Tolerance for Applications/Workloads Protected Cloud-based Backup Services



Source: Enterprise Strategy Group, 2013.

The importance of protecting data is also evident based on the frequency with which backup copies are made. As shown below, while more than one-quarter (27%) of current BaaS users say they back up data at least once every hour (if not more frequently), nearly half (45%) make copies no more than once daily (see Figure 17). In today's IT environments, where data has high value and organizations have a low tolerance for downtime, protecting it on just a daily basis seems dangerous. Instead, using the earlier recommendation of an on-premises appliance as part of the solution architecture, one should be protecting data multiple times per day (at least between the production and on-premises protection servers), and then replicating to the BaaS repository as often as is viable.

Figure 17. Frequency of Backup Copies for Applications/Workloads Protected by Cloud-based Backup Services



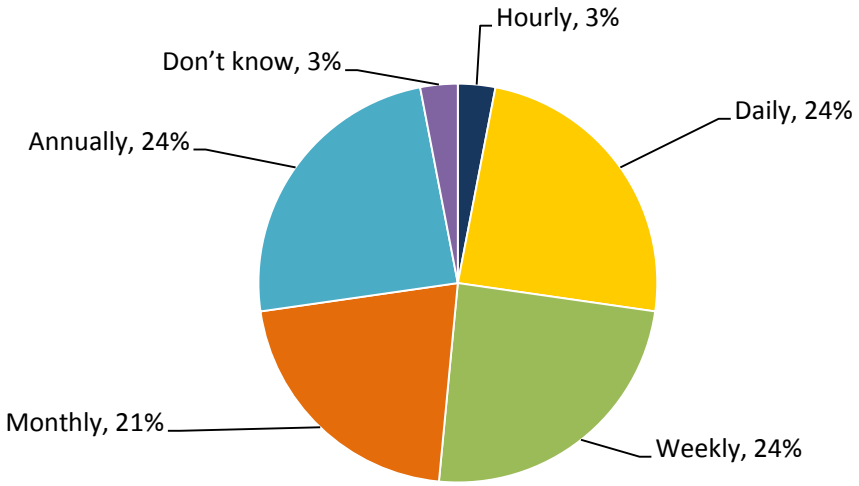
Source: Enterprise Strategy Group, 2013.

Backing up data is only half of the data protection paradigm since it's ultimately about *getting the data back* when necessary. Indeed, conversations with backup administrators will often include the occurrence of calls from employees asking for help counteracting a lost or deleted file. When asked how frequently IT staff typically retrieves BaaS-resident backup data—whether a deleted, lost, or damaged file—from its provider, current cloud-based service users were pretty evenly split between those identifying this as a daily, weekly, monthly, or annual activity (see Figure 18). It is worth pointing out that these data retrievals imply both data recoveries due to actual incidents and data retrievals caused by a testing process or other operational administrative task.

While a mere 3% of current users indicate an hourly cadence when retrieving backup data from BaaS repositories, the consideration that 27% are interfacing with their backup solutions on at least a daily basis reinforces ESG's belief that a more rapid restore capability via an on-premises device within the BaaS solution is important.

Figure 18. Frequency of Backup Data Retrievals from Cloud-based Backup Service Providers

How frequently does your organization's IT staff typically retrieve backup data (i.e., file(s) accidentally deleted, lost, damaged, etc.) from its BaaS service provider? (Percent of respondents, N=29)

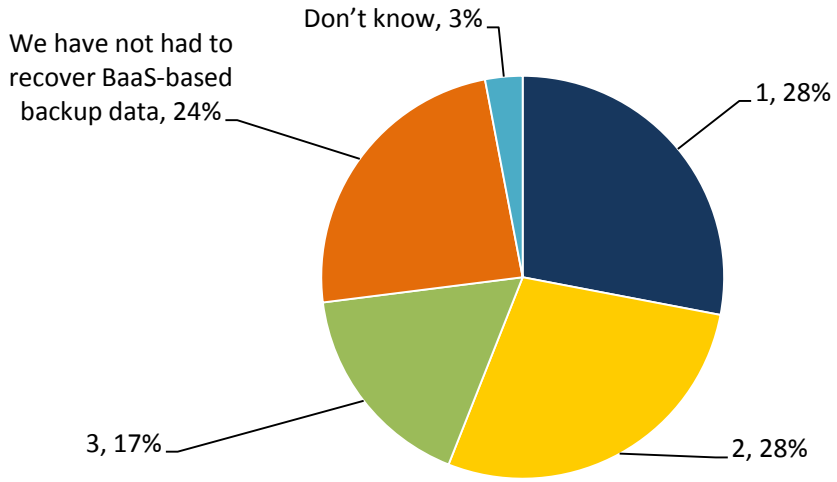


Source: Enterprise Strategy Group, 2013.

In terms of more significant data recovery efforts (i.e., a larger data set than simply a single file), nearly one-quarter (24%) of current BaaS users report that their organizations have not yet had to go through such a process (see Figure 19). It is worth noting that not a single current BaaS user has had to undertake a large data recovery operation more than three times since the inception of their organizations' service usage.

Figure 19. Frequency of Backup Data Recoveries from Cloud-based Backup Service Providers

How many times within the last year has your organization had to recover (i.e., more than just a single file) data from its BaaS service provider? (Percent of respondents, N=29)

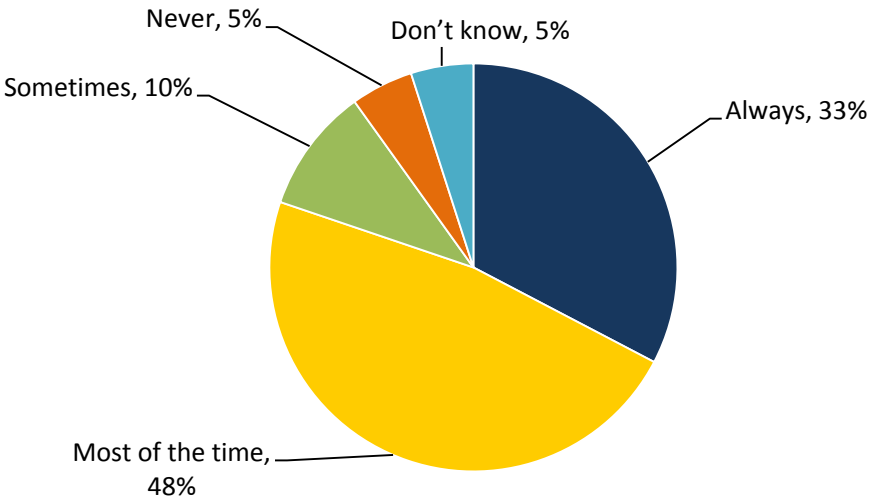


Source: Enterprise Strategy Group, 2013.

Those organizations that have had to recover data from their BaaS providers were then asked about their success rate(s). As seen in Figure 20, only one-third claims that their recovery time objectives have always been achieved.

Figure 20. Rate of Successful Data Recoveries

In those cases that your organization has had to recover data, were your recovery time objectives (RTOs) met successfully? (Percent of respondents, N=21)



Source: Enterprise Strategy Group, 2013.

Despite the fact that network bandwidth continues to become more widely available, attempting a significant data recovery operation (i.e., more than a single file) over the wire is not necessarily feasible. In order to compensate for network shortcomings and/or difficulties (i.e., cost), many BaaS providers offer some type of workaround to help with bulk restores. When asked which approach is provided with their service, 41% of current BaaS users say an

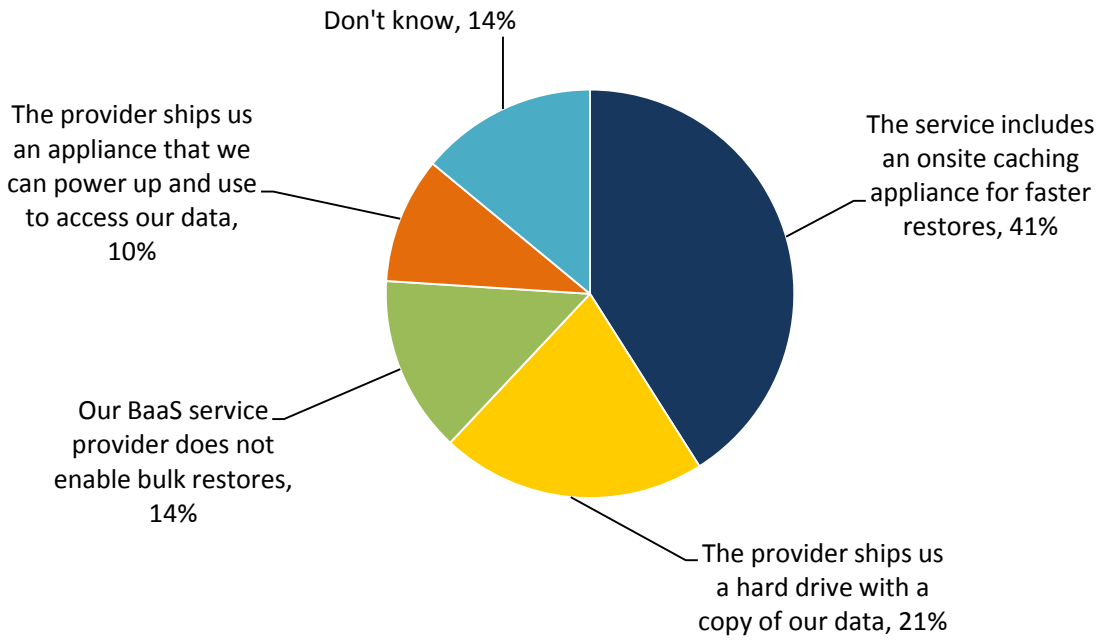
onsite caching appliance is included for faster restores (see Figure 21). Nearly one-third report receiving either a hard drive with a copy of their data (21%) or an appliance that can be used to access data (10%).

It is worth drawing attention to the fact that more than one-quarter (28%) of current BaaS users claim that either their service provider does not offer a bulk restore option or they are not aware of such a capability. This is a key differentiation point among BaaS solutions. While only some BaaS solution providers offer a form of mass-ingest of data (often by sending a hard drive of data), even fewer of them offer this capability for a restore. Without it, users may be surprised at the number of days it takes to perform the restoration of a data set of any appreciable worth.

With so much critical data—as evidenced by the reported downtime requirements of hours or less—ESG believes that most cloud-based BaaS architectures will continue to require an on-premises appliance or other backup device as part of the solution. This allows data to quickly leave the production server to the onsite device, particularly for frequently protected systems. In addition, with downtime tolerance being so low, rapid restores of large data sets seem nonviable. Thus, an on-premises capability for more rapid restores (while most previous versions will be in the cloud copy) seems a requirement for data sets of any size.

Figure 21. Bulk Restore Options Offered by BaaS Service Providers

How does the BaaS service provider that your organization uses allow for bulk restores of large amounts of data? (Percent of respondents, N=29)



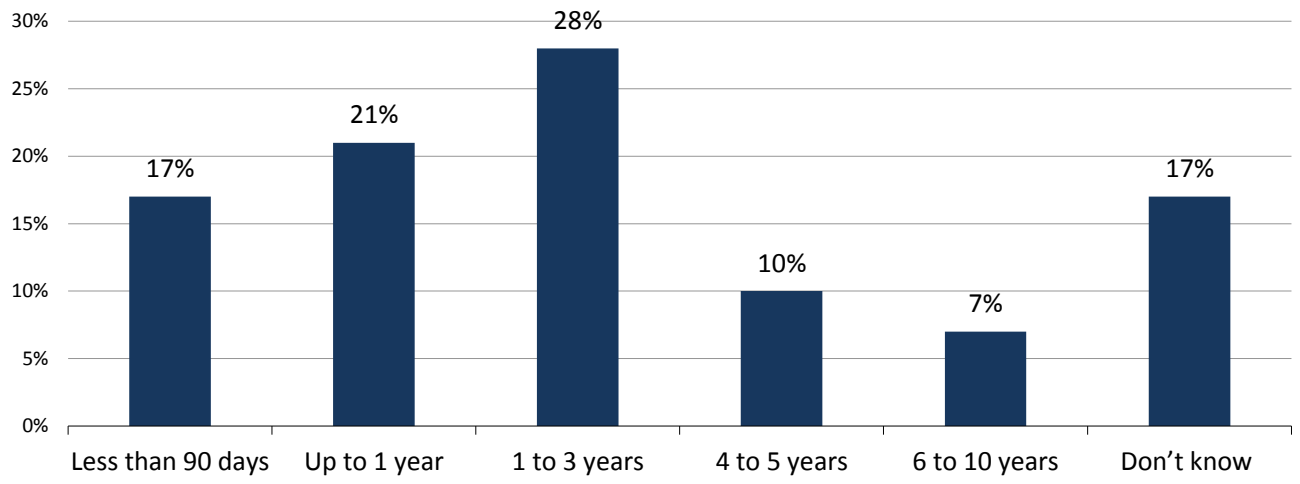
Source: Enterprise Strategy Group, 2013.

What impact does BaaS have on the length of time organizations retain backup data? In order to establish a baseline, respondent organizations were asked about retention in the context of all the data they protect. As seen in Figure 46 in the *Respondent Demographics* section, nearly two-thirds (64%) do not retain backup data for more than three years, which is comparable with current BaaS users that report that their service providers don't exceed retention periods of three years (see Figure 22). However, backup data in general is three times likelier than cloud-based backup data (24% vs. 7%) to be stored for at least six years, and not a single user of cloud-based backup services claims that her provider stores data for a period of more than ten years.

Could BaaS providers stand to benefit from increasing the amount of time they store customers' backup data? Current cloud backup users were asked if increased retention times of secondary and tertiary data would affect their usage of these services. As seen in Figure 23, nearly two-thirds (62%) of current BaaS users believe they would use cloud-based services to protect more applications/data if their provider offered longer-term retention.

Figure 22. Typical Data Retention Time Provided by BaaS Service Providers

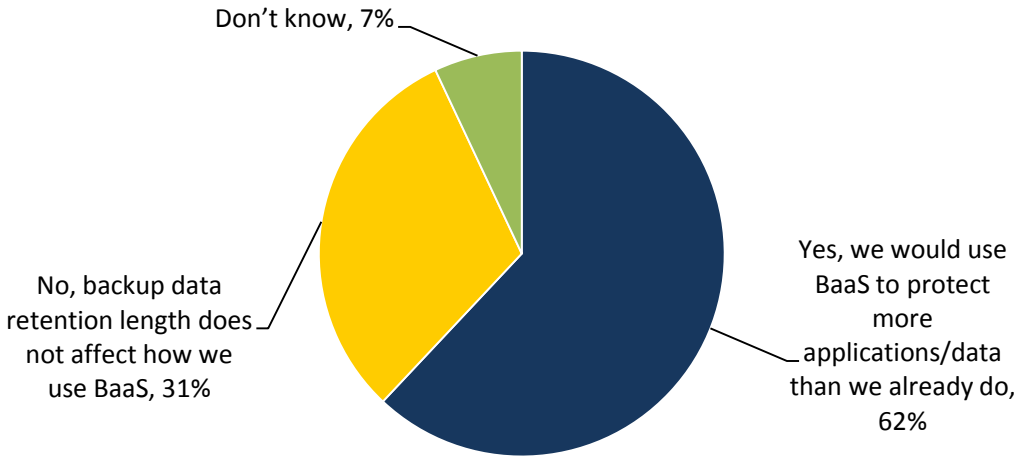
To the best of your knowledge, for what length of time is your organization's BaaS-based backup data typically retained? (Percent of respondents, N=29)



Source: Enterprise Strategy Group, 2013.

Figure 23. Potential Impact of Increased Backup Data Retention Time on BaaS Usage

If your BaaS provider offered longer-term retention of backup data, would that affect your organization's usage of that type of service? (Percent of respondents, N=29)



Source: Enterprise Strategy Group, 2013.

Disaster Recovery-as-a-service (DRaaS) Usage Trends

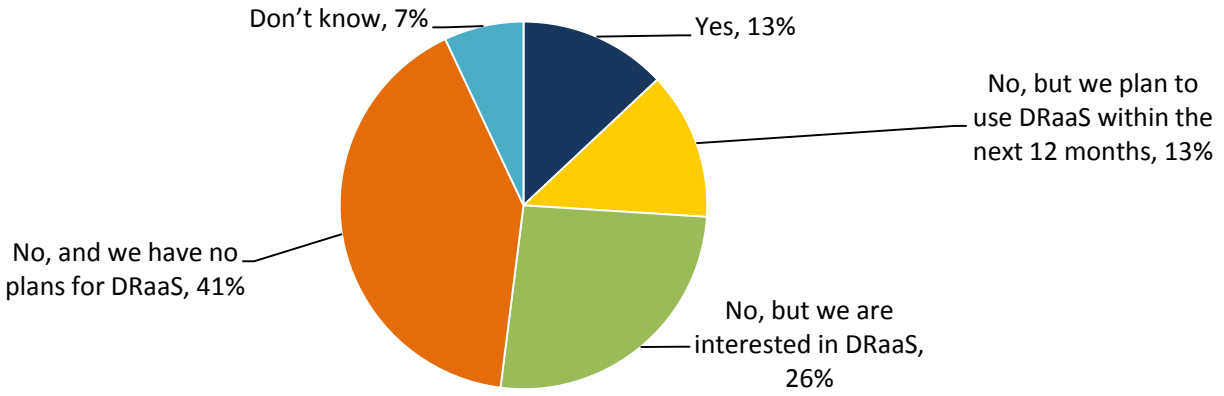
In order to gauge adoption levels for cloud-based disaster recovery services, ESG asked respondents if any of their physical servers and/or virtual machines are protected via the DRaaS model. For the purposes of this report, disaster recovery-as-a-service was defined as follows:

> *Third-party service that provides a means for whole servers, virtual machines, or applications (i.e., services) to be replicated to the cloud. In the event of a crisis, those servers or virtual machines can resume operation from the cloud provider, without having to first be restored to the on-premises data center. Backup of the individual files/data may not be included, but the primary function is the ability to resume services from the cloud.*

According to Figure 24, only 13% of survey respondents currently use DRaaS to protect servers and/or virtual machines, while an additional 40% have plans for or interest in these cloud-based disaster recovery services.

Figure 24. Usage Trends for Disaster Recovery-as-a-service (DRaaS)

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=306)



Source: Enterprise Strategy Group, 2013.

As was the case with DPaaS in general and BaaS specifically, organizations with larger data protection budgets are most likely to be currently using or open to the possibility of using DRaaS. Specifically, Table 3 reveals that organizations spending less than $100,000 annually on data protection-related expenses are significantly more likely than those with budgets of at least $1 million in a typical year to have *no* plans for or interest in cloud-based disaster recovery services (53% vs. 34%).

Table 3. Usage Trends for Disaster Recovery-as-a-service (DRaaS), by Typical Annual Data Protection Budget

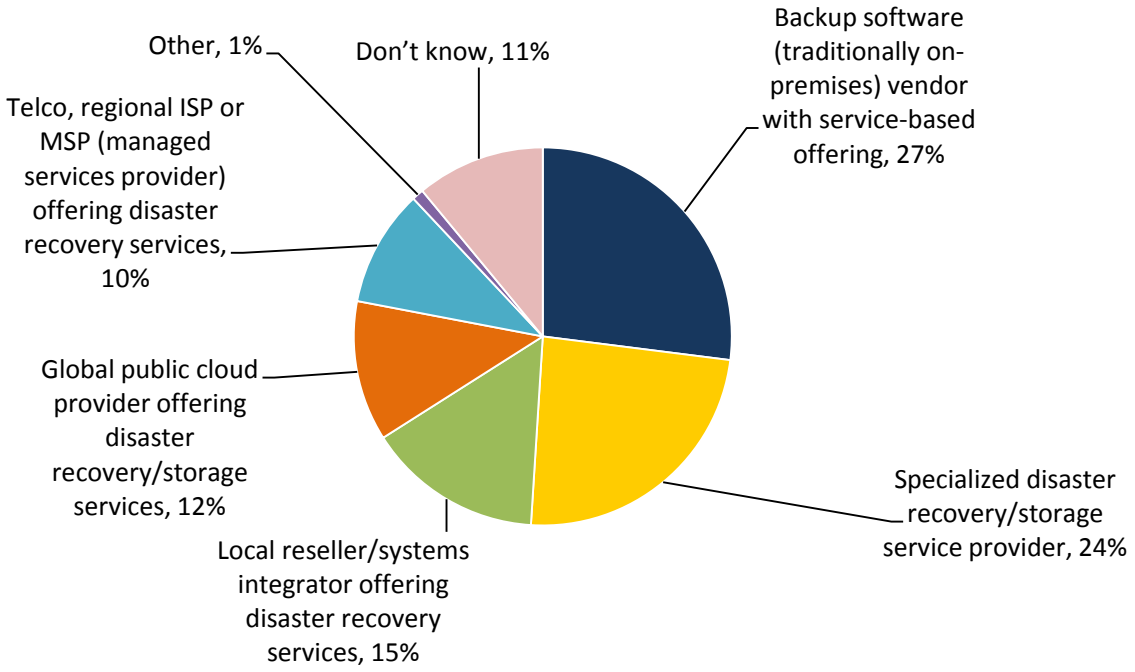
Is your organization currently using disaster recovery-as-a-service (DRaaS) to protect any of its servers and/or virtual machines (VMs)?			
	By typical annual data protection budget		
	Less than $100,000 (N=78)	$100,000 to $999,999 (N=108)	$1m or more (N=79)
Yes	13%	11%	20%
No, but we plan to use DRaaS within the next 12 months	6%	20%	15%
No, but we are interested in DRaaS	28%	27%	30%
No, and we have no plans for DRaaS	53%	42%	34%
TOTAL	**100%**	**100%**	**100%**

Source: Enterprise Strategy Group, 2013.

Current and potential DRaaS users were then asked to identify the source from which they purchase–or expect to purchase–cloud-based disaster recovery services. As seen in Figure 25, more than half of these organizations procure these services–or expect to do so–from either traditional backup software vendors (27%) or specialized disaster recovery/storage service providers (24%). Similar trends exist in terms of procurement sources for DRaaS and BaaS (as seen in Figure 10) in that customers are recognizing that a key to their own success is partnering with providers that not only offer better economics and technical capabilities, but also possess experience in data protection services. In so doing, the service provider is more likely to keep the data protection software (including any agents at customer sites) running reliably, and remaining more agile and dependable for recoveries.

Figure 25. Source from Which Current and Potential DRaaS Users Purchase or Expect to Purchase Cloud-based Disaster Recovery Services

From which of the following sources does your organization purchase – or expect to purchase – a DRaaS solution? (Percent of respondents, N=159)

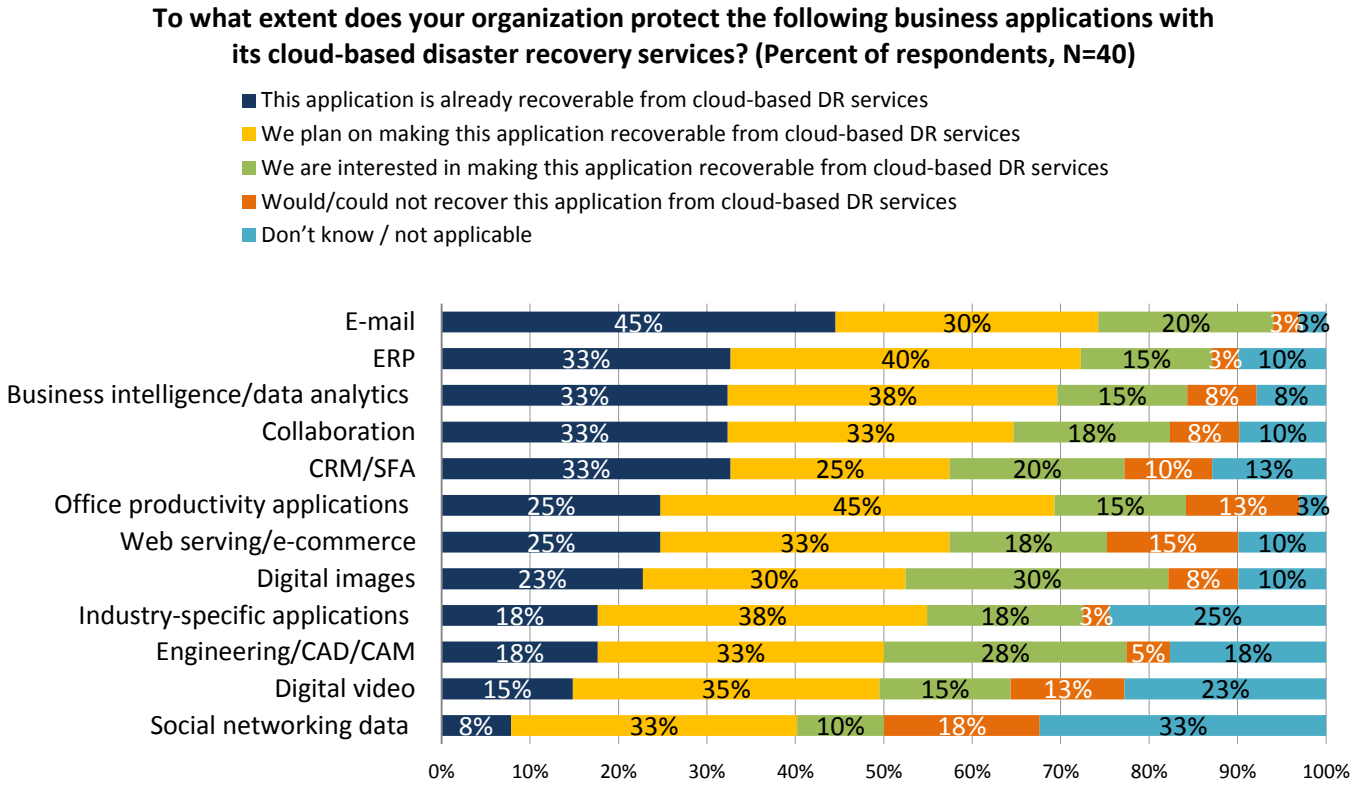


Source: Enterprise Strategy Group, 2013.

There is not much difference between which applications current users would protect with DRaaS (see Figure 26), versus BaaS (as seen previously in Figure 13). And although it is a reasonable strategy, one might wonder whether "failing over" from production to cloud-based DR sites is the most effective approach, especially when compared with hybrid data availability architectures, such as SQL database mirroring between sites.

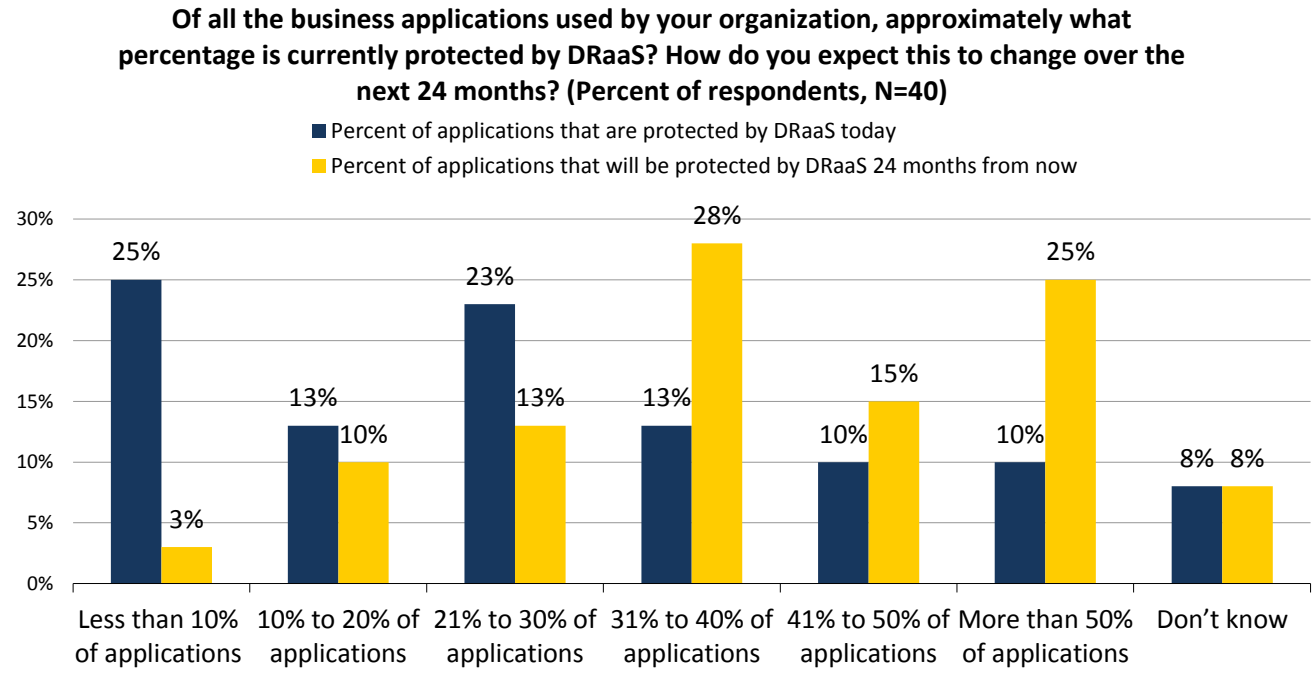
ESG also sees similar inclinations between current and potential use of BaaS and DRaaS in terms of the extent of total applications protected (see Figure 27). This is encouraging as IT organizations discover DPaaS offerings and then evolve from BaaS to DRaaS (or vice versa).

Figure 26. Applications Current DRaaS Users Protect with Cloud-based Disaster Recovery Services



Source: Enterprise Strategy Group, 2013.

Figure 27. Extent of DRaaS Usage, Now and 36 Months from Now

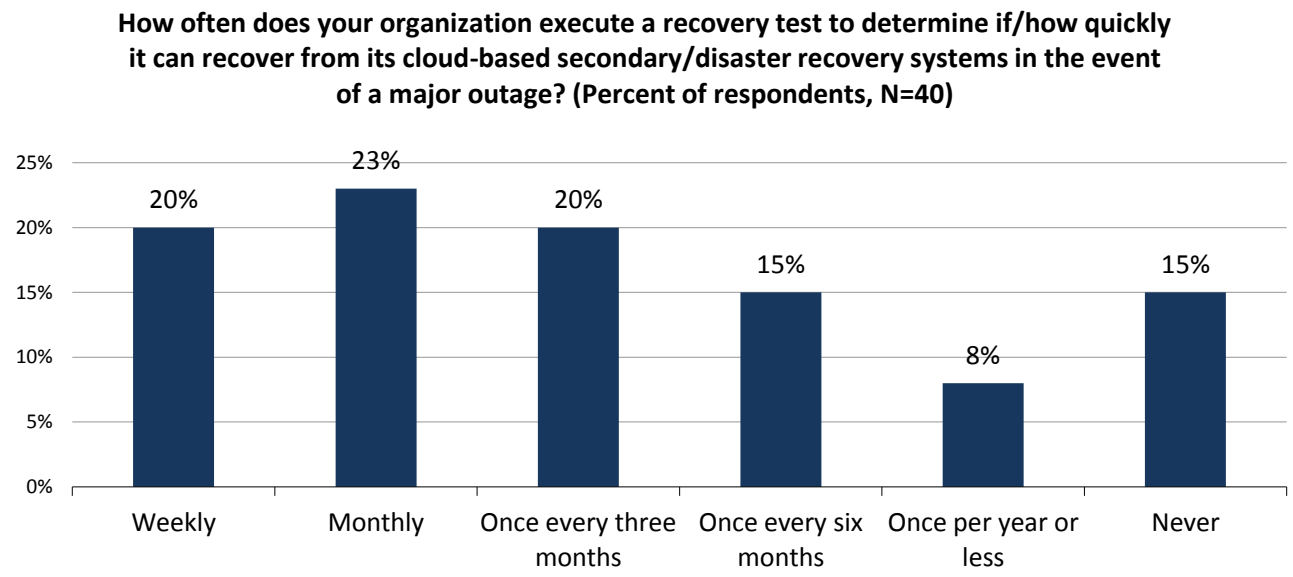


Source: Enterprise Strategy Group, 2013.

One of the primary challenges with most BC/DR plans is that recurring testing must occur in order to ensure preparedness for when calamity strikes and to prove compliance for those with regulatory mandates. But testing in general can be arduous and risky—arduous in the complexity of bringing replacement systems online, perhaps without the consistency of patches or other operational maintenance until the test; risky in that bringing those systems online carries the possibility of affecting the original servers, which are serving customers.

When asked about the frequency of disaster recovery testing from cloud-based secondary systems, 43% of current DRaaS users report doing so on a weekly (20%) or monthly (23%) basis (see Figure 28). This is especially significant when compared with the frequency of testing within a self-hosted BC/DR plan, specifically the fact that users of cloud-based DR services are more than three times as likely as those taking the do-it-yourself (DIY) approach (20% vs. 6%) to perform weekly recovery tests to determine if and how quickly they could recover from a major outage (see Table 4).

Figure 28. Frequency of Disaster Recovery Testing from Cloud-based Secondary Systems



Source: Enterprise Strategy Group, 2013.

Table 4. DRaaS Fosters More Frequent Disaster Recovery Testing

How often does your organization execute a recovery test to determine if/how quickly it can recover from its secondary/disaster recovery systems in the event of a major outage?		
	By current DR model	
	Self-hosted (N=252)	Cloud-based (N=40)
Weekly	6%	20%
Monthly	17%	23%
Once every three months	19%	20%
Once every six months	17%	15%
Once per year or less	31%	8%
Never	10%	15%
TOTAL	**100%**	**100%**

Source: Enterprise Strategy Group, 2013.

Usage of Cloud Storage Services (STaaS) to Store Backup Data

Some cloud-based data protection services exist simply to provide remote/offsite capacity on which to store copies of backup data. In addition to data-center-resident applications and systems, a growing number of use cases require some type of backup strategy, whether it's the proliferation of alternative endpoint devices like smartphones and tablet computers stemming from bring-your-own-device (BYOD) policies or the increased number of mobile and remote employees. For the purposes of this report, cloud storage services for backup data were defined as follows:

> *Third-party service that supplements a traditional backup solution—meaning a backup application that operates on-premises and makes copies of data to local/onsite media (such as tape, disk, etc.)—with a cloud-based storage service (i.e., capacity in the cloud) in order to have an offsite copy of the data that leverages cloud economics. This does not include cloud-based backup services with an on-premises caching appliance (i.e., this is not synonymous with BaaS).*

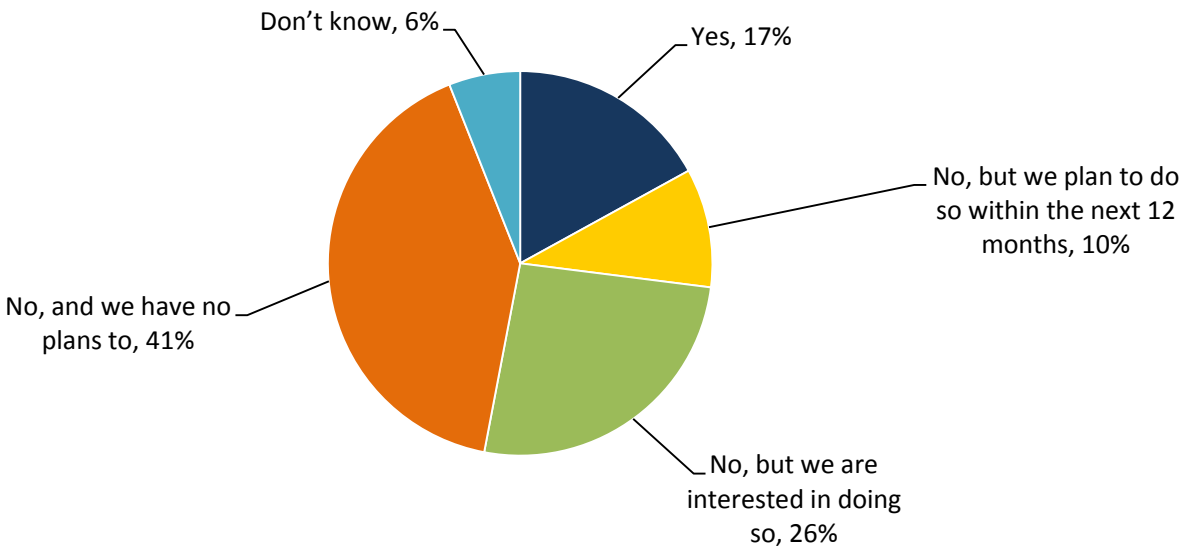
To be clear, BaaS with an on-premises recovery appliance can look *very* similar to a STaaS-extended, on-premises solution. However:

- BaaS solutions are delivered with a cloud-centric management and deployment model, with the intermediary recovery appliance often being optional in theory—though mandatory in practice.
- STaaS solutions are just an extension of the on-premises backup solution, which is mandatory, by providing additional capacity or alternate capability that simply resides in the cloud.

In terms of adoption trends, nearly one-in-five (17%) respondent organizations currently use cloud storage services as an offsite repository for backup data (see Figure 29). These numbers are consistent with previously conducted ESG research that revealed backup data to be the most common use case for third-party storage capacity.[6]

Figure 29. Usage of Cloud Storage Services (STaaS) to Store Backup Data

Is your organization currently using cloud storage services to store any of its backup data? (Percent of respondents, N=306)



Source: Enterprise Strategy Group, 2013.

As was the case with the other cloud-based data protection models, larger organizations—as measured by annual data protection spending—were significantly more likely to currently use offsite capacity for their backup data or at least be open to the idea of doing so (see Table 5).

[6] Source: ESG Research Report, *2012 Public Cloud Computing Trends*, March 2012.

Table 5. Usage of Cloud Storage Services (STaaS) to Store Backup Data, by Typical Annual Data Protection Budget

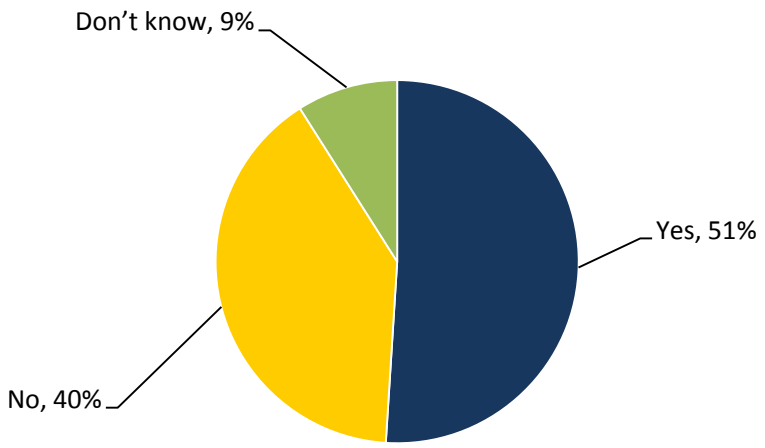
Is your organization currently using cloud storage services to store any of its backup data?			
	By typical annual data protection budget		
	Less than $100,000 (N=79)	$100,000 to $999,999 (N=109)	$1m or more (N=78)
Yes	14%	17%	24%
No, but we plan to use STaaS within the next 12 months	5%	13%	15%
No, but we are interested in STaaS	25%	26%	29%
No, and we have no plans for STaaS	56%	44%	31%
TOTAL	**100%**	**100%**	**100%**

Source: Enterprise Strategy Group, 2013.

One of the most disappointing revelations of the research was the fact that barely half (51%) of those respondents using cloud-based storage to store backup data believe that their on-premises backup solutions are actually compatible with these services (see Figure 30). If true, this speaks to the sluggish rate at which backup software vendors are evolving to take advantage of cloud storage. It is more likely, however, that IT respondents are unaware of whether or not their backup software is cloud-extensible. This may be because they never asked the question or vendors have failed to effectively communicate this capability, particularly to existing customers who may not have been exposed to newer features to which they are entitled.

Figure 30. Support of Cloud Storage Services by On-premises Backup Application

Does your on-premises backup application support cloud storage services? (Percent of respondents, N=162)



Source: Enterprise Strategy Group, 2013.

Conclusion

Arguably, nothing has affected the re-imagination of IT as much as cloud-based services. And of the many IT infrastructure services that could be delivered from the cloud, data protection is often perceived as one of the first to embrace. But which one?

- Backing up data to the cloud to reduce infrastructure and improve restorability via BaaS
- Replicating VMs to the cloud to ensure business continuity by spinning the VMs up when needed via DRaaS
- Extending on-premises backup solutions with cloud-based capacity for broader data protection via STaaS

Regardless of the method, a few key ideas ring true:

Current and potential DPaaS users are looking to specialized backup/disaster recovery service providers, as well as services that are owned and operated by the ("traditional") backup/DR software vendors that they deal with today, for cloud-based data protection capabilities. By correctly recognizing that a cloud-based service is simply a method of delivering IT functionality, customers are rightfully expecting that any potential service provider would have notably more data protection experience than their own IT departments. Thus, telcos/ISPs, public cloud providers, and local resellers should evolve into DPaaS providers at their own discretion and with that understanding.

Those providers may wish to consider developing services to provide monitoring capabilities instead. As part of these offerings, subscribers would not have to change from their existing BaaS or on-premises backup solutions, but they would gain the benefit of an experienced remote support person to monitor the health of their backup systems—regardless of their location—and resolve issues when they come up.

Beyond the common themes, a few other implications of the data include:

- **BaaS** solutions need to store data longer and cheaper (which will increase adoption usage), with disk-to-disk-to-cloud (D2D2C) capabilities a must for most environments. Additionally, a local recovery capability—whether in the form of an appliance, disk driver, server, etc.—acting as an intermediary between the production servers and the cloud service would not only provide for faster recovery, but would also create a second copy that is unbuffered for immediate protection out of the production server itself.
- **DRaaS** is effective and appealing from an OPEX/CAPEX perspective for use in an organization's overall data protection strategy. Perhaps most encouraging is the significantly higher test rates by DRaaS users over onsite "do-it-yourself" DR solutions. Without the need for redundant hardware, there is very little economic impact to testing aspects of the DR solution set. And more frequent testing will reveal more kinks in the plan, which will increase the likelihood of success when recovery operations are actually necessary.
- **STaaS** is seeing even better adoption than BaaS/DRaaS, presumably because adding cloud storage to an otherwise established solution is less invasive than completely replacing entrenched data protection products and processes.

Research Implications for Data Protection Vendors and DPaaS Providers

This research is reflective of the rapidly evolving range of data protection services that are available today. Almost every customer is considering the cloud for at least part of his data protection strategy, but it is not so simple to switch. As such, data protection vendors should:

- **Understand that BaaS/DRaaS isn't the answer for everyone**. Many customers are perfectly happy with their on-premises backup and/or disaster recovery solutions, while still wanting to embrace the cloud for data survivability purposes. As such, "traditional" data protection vendors should not only ensure that their solutions are cloud extensible, but make this abundantly clear to customers through marketing awareness, technical documentation, and third-party assessments/endorsements.

- **Recognize that some customers have longer data retention requirements.** Certain potential BaaS customers will not be able to fully embrace offerings that do not offer the length of data retention their organizations require. Services that cannot yet meet these requirements can compensate by considering open media standards (e.g., LTFS on LTO) or exportable data sets on disk for flexibility, which could potentially win over customers who are looking for longer retention standards.
- **Realize that agility for restoration and testing are the differentiators for DRaaS solutions…** This includes sandboxing for restoring interdependently linked VMs, such as Active Directory, front-end web servers, and a back-end database. Without sandboxing, for test and for real production environments, the potential of DRaaS will be lacking.
- **…while DPaaS providers need to offer better ingestion methods and recovery mediums.** This includes shipping disk drives (BaaS) or hypervisor appliances (DRaaS) in order to make onboarding and massive recovery scenarios more viable.
- **Know that endpoint device protection is the future, with BYOD as the driving force.** Corporate data resides on mobile devices—and they, therefore, require protection by IT (and not just by the users). Without corporate-provided backups, technology-savvy users will circumvent IT and do their own backups. And at the end of those employees' time with the company, they will walk out of the building with their device (and its data) and all of the backups that they completed themselves.

Research Implications for IT/Data Protection Professionals

While many IT environments will invariably have some type of cloud-service as part of its overall delivery plan moving forward, it is important to recognize that cloud-based methods are just that: a method of delivering IT services. And just like any other IT method, its applicability will vary greatly from "hardly applicable" to "hugely beneficial." To that end, be clear why/whether BaaS is applicable to your server and endpoint workloads. For example, laptops, including those that are part of a BYOD initiative and those that are companyowned, may be well suited for BaaS, but server data may not be.

Retention Considerations

Endpoint protection tends to be for a shorter retention period (months or less), while server data may have a retention requirement of five or more years (which is beyond what most BaaS providers offer today). If your retention requirements exceed your BaaS providers' offerings, either consider changing BaaS providers or consider this:

- You will almost assuredly have an on-premises ***disk*** appliance for faster/larger recoveries.
- Without a long-term BaaS service, you may still be required to maintain ***tapes*** for retention purposes.
- With disk for short-term recovery and tape for long-term retention, what role will the ***cloud*** copy play in your strategy?

Usability Considerations

How do you need to access the cloud copy(s) of the data?

- If the cloud is simply a repository extension, then cloud-based storage for your existing on-premises solution may be satisfactory. This is important to be clear about because cloud storage will appear as either iSCSI blocks or an NFS/CIFS file system simply holding "backup data," meaning that the data is unusable without the backup server connected.
- If the cloud copy is intended for file- or object-centric data restores, either a BaaS solution or a cloud-enhanced on-premises solution may be equally applicable (assuming the data is accessible from the cloud repository through a web-UI).

- If applications or services need to be restarted, plan on DRaaS over BaaS/STaaS, whereby virtual machines or other packaged application models can be protected and replicated between their primary (typically on-premises) locations to a cloud service that is capable of hosting/launching the VMs or services.

Topology Considerations

As with every other data protection strategy decision, the answer will always be "it depends," until you have clearly defined the question: "What types of recoverability does the organization require?"

- *For laptops* that seldom connect to the corporate network yet typically see the Internet, the cloud appears to be the right answer for most, with follow-on questions related to IT manageability compared with user-experience.
- *For data center data* where a second facility already exists, cloud scenarios are more ambiguous and will often be considered in the context of BC/DR goals, current operational models, and retention requirements.
- *For everything in between* (such as remote/branch offices) considerations such as the difference between Internet access and Intranet access will come into play, as will considering how centralized the rest of the corporate IT management function is, both technically and culturally.

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 May 3, 2013 and May 10, 2013. To qualify for this survey, respondents were required to be IT professionals responsible for data protection technology decisions for their organizations. 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 306 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.

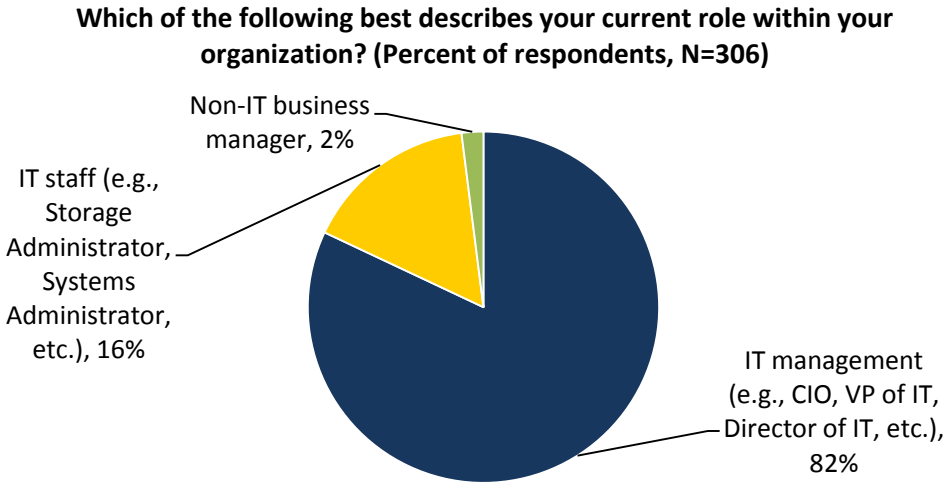
Respondent Demographics

The data presented in this report is based on a survey of 306 qualified respondents. The figures below detail the demographics of the respondent base, including individual respondents' current job responsibility, responsibility for data protection technologies, and primary area of technology responsibility, as well as respondent organizations' total number of employees, total number of employees responsible for data protection, primary industry, annual revenue, annual amount spent on data protection technologies, specific areas of data protection spending, age of respondents' organization, number of physical servers deployed, use of server virtualization, total storage capacity, and annual data storage growth rate.

Respondents by Current Responsibility

Respondents' current responsibility within their organizations is shown in Figure 31.

Figure 31. Survey Respondents by Current Responsibility

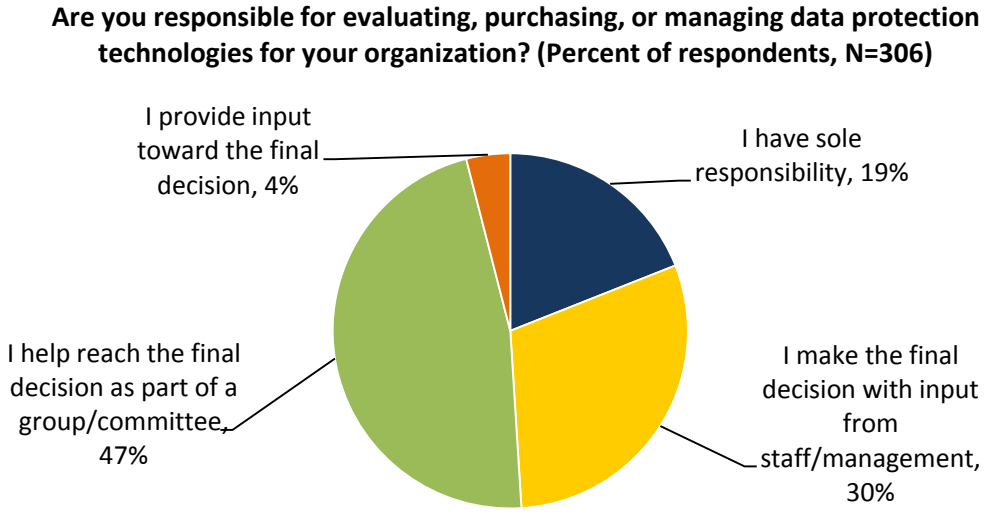


Source: Enterprise Strategy Group, 2013.

Respondents by Data Protection Technology Responsibility

Respondents' current responsibility with regards to data protection technologies is shown in Figure 32.

Figure 32. Survey Respondents by Data Protection Technology Responsibility



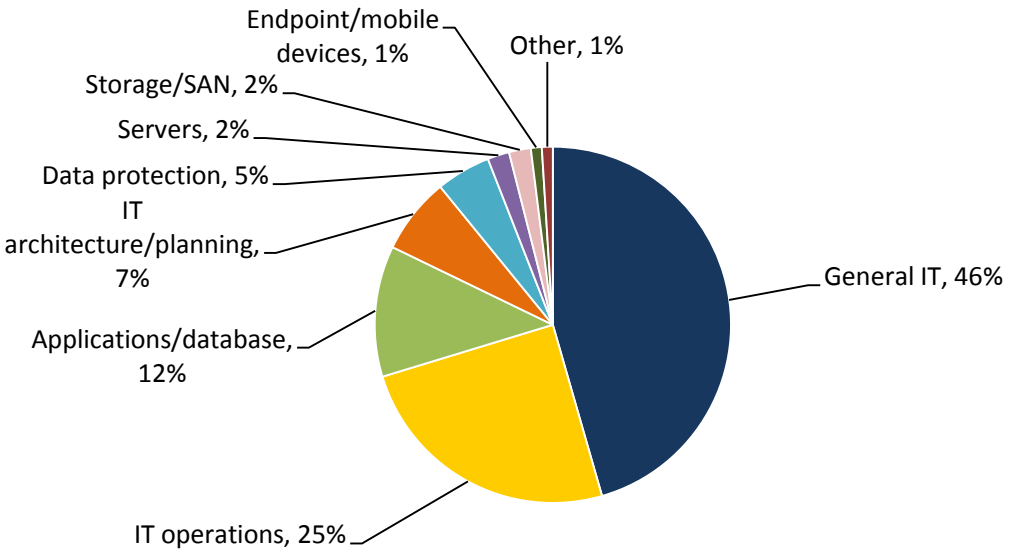
Source: Enterprise Strategy Group, 2013.

Respondents by Primary Area of Technology Responsibility

Respondents' current primary area of technology responsibility is shown in Figure 33.

Figure 33. Survey Respondents by Primary Area of Technology Responsibility

Which of the following would you consider to be your primary area of technology responsibility? (Percent of respondents, N=306)



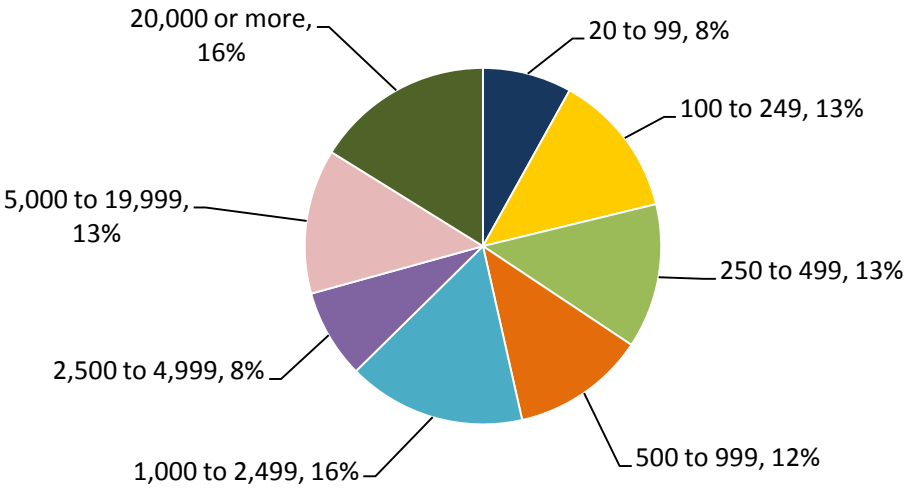
Source: Enterprise Strategy Group, 2013.

Respondents by Number of Employees

The number of employees in respondents' organizations is shown in Figure 34.

Figure 34. Survey Respondents by Number of Employees

How many total employees does your organization have worldwide? (Percent of respondents, N=306)



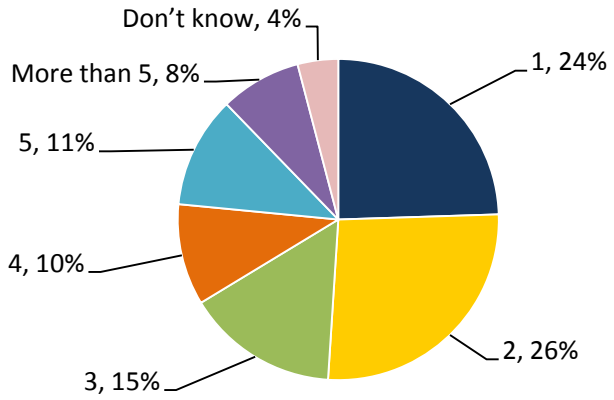
Source: Enterprise Strategy Group, 2013.

Respondents by Number of Employees Responsible for Data Protection

The number of employees responsible for managing the data protection environment in respondents' organizations is shown in Figure 35.

Figure 35. Survey Respondents by Number of Employees Responsible for Data Protection

Approximately how many administrators (measured in FTEs – full-time equivalents) are responsible for managing your organization's data protection environment? (Percent of respondents, N=306)



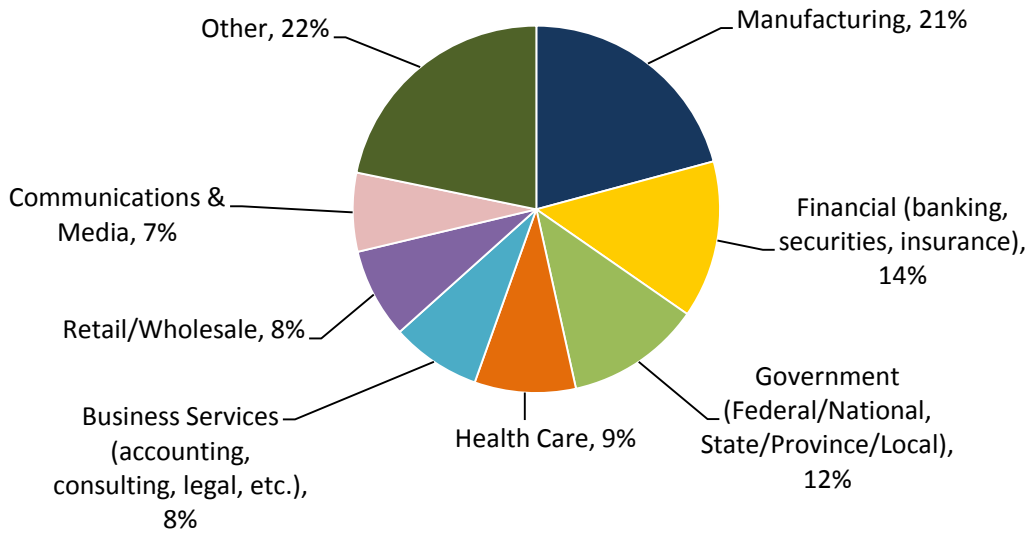
Source: Enterprise Strategy Group, 2013.

Respondents by Industry

Respondents were asked to identify their organizations' primary industry. In total, ESG received completed, qualified respondents from individuals in 19 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 36.

Figure 36. Survey Respondents by Industry

What is your organization's primary industry? (Percent of respondents, N=306)

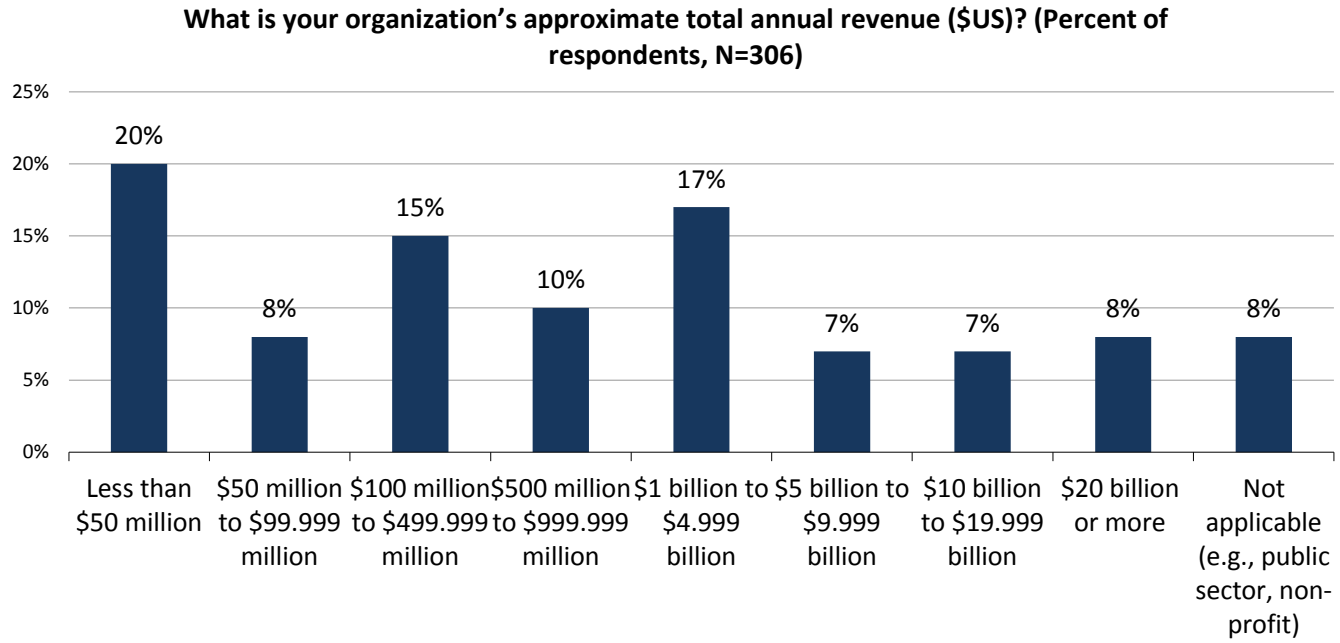


Source: Enterprise Strategy Group, 2013.

Respondents by Annual Revenue

Respondent organizations' annual revenue is shown in Figure 37.

Figure 37. Survey Respondents by Annual Revenue

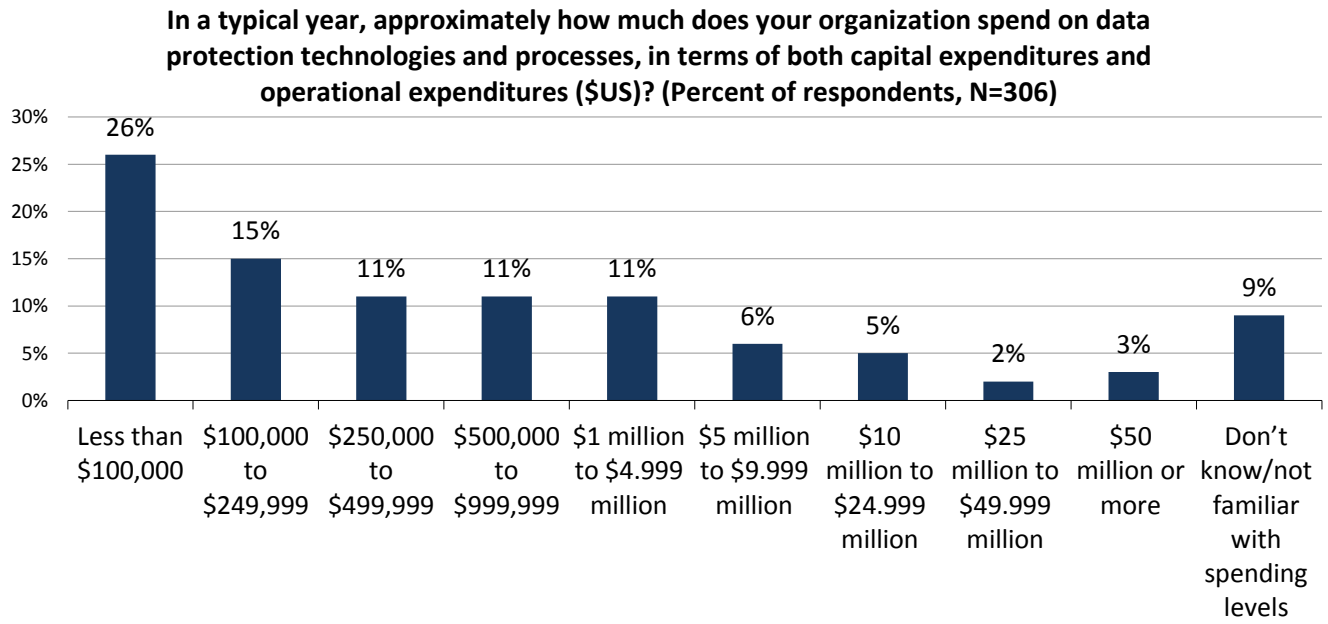


Source: Enterprise Strategy Group, 2013.

Respondents by Data Protection Spending

The amount respondent organizations typically spend annually on data protection technologies and processes (including capital and operational expenditures) is shown in Figure 38.

Figure 38. Survey Respondents by Data Protection Spending

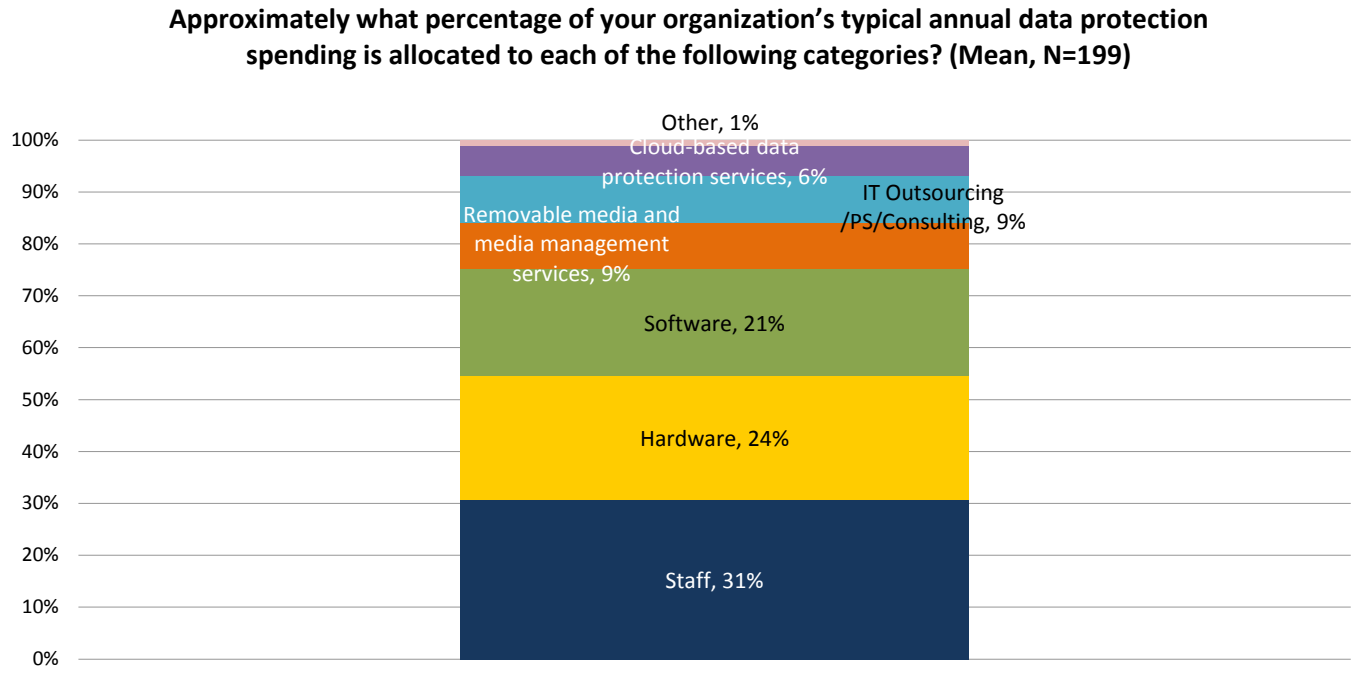


Source: Enterprise Strategy Group, 2013.

Respondents by Data Protection Spending Technology Profile

The growth rate for total volume of data at respondent organizations is shown in Figure 39.

Figure 39. Survey Respondents by Annual Growth Rate

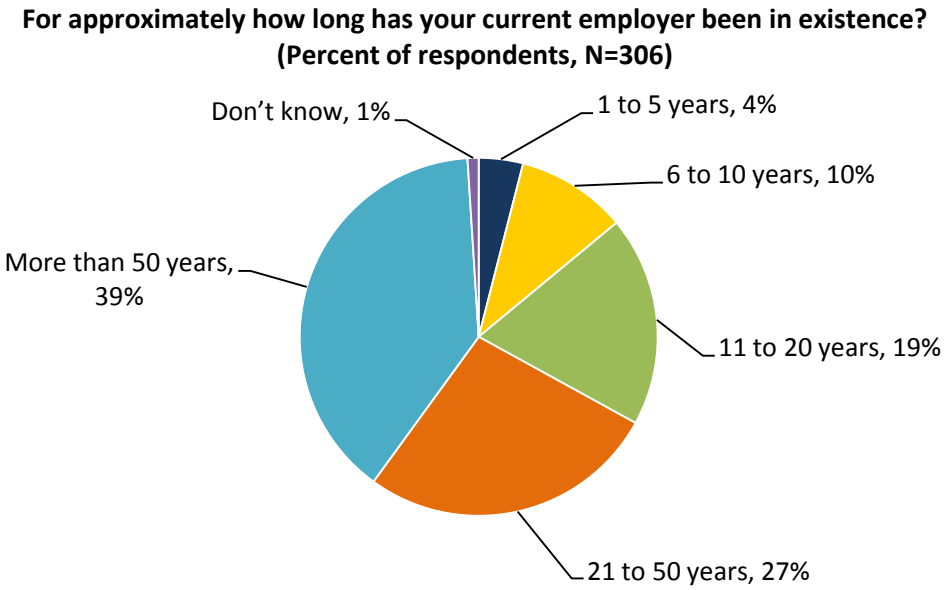


Source: Enterprise Strategy Group, 2013.

Respondents by Age of Organization

The length of time a respondent's employer has been in existence is shown in Figure 40.

Figure 40. Survey Respondents Age of Organization

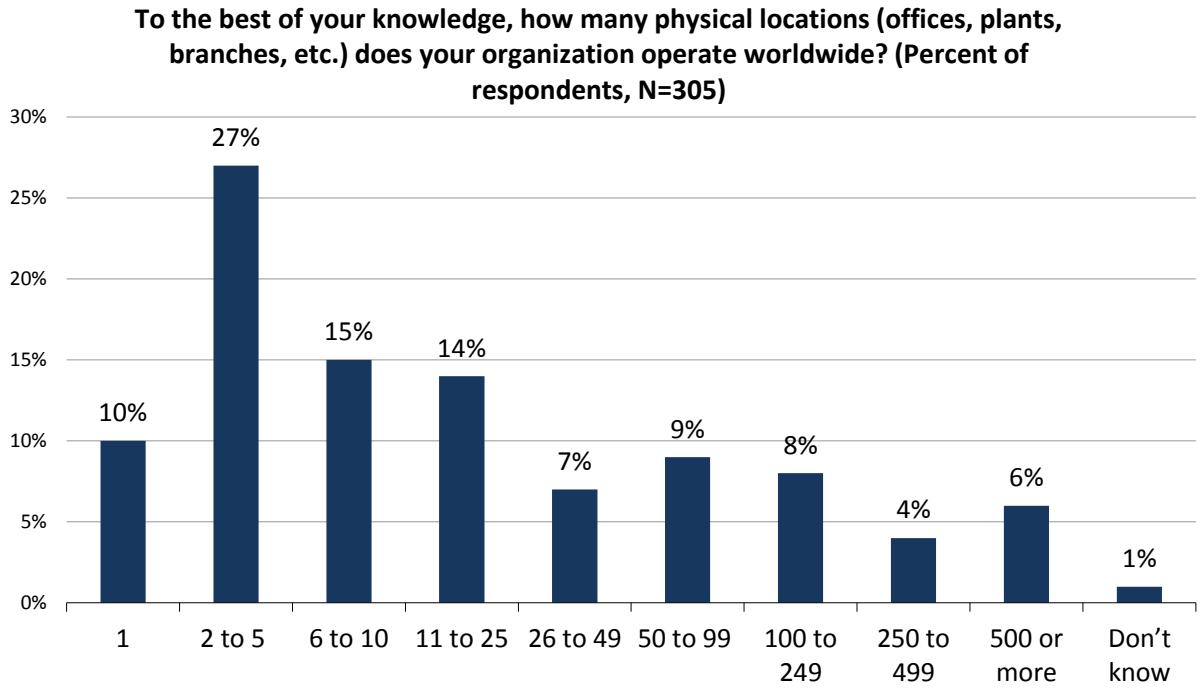


Source: Enterprise Strategy Group, 2013.

Respondents by Number of Physical Locations

The number of physical locations (offices, plants, branches, etc.) respondent organizations operate worldwide is shown in Figure 41.

Figure 41. Survey Respondents by Number of Physical Locations

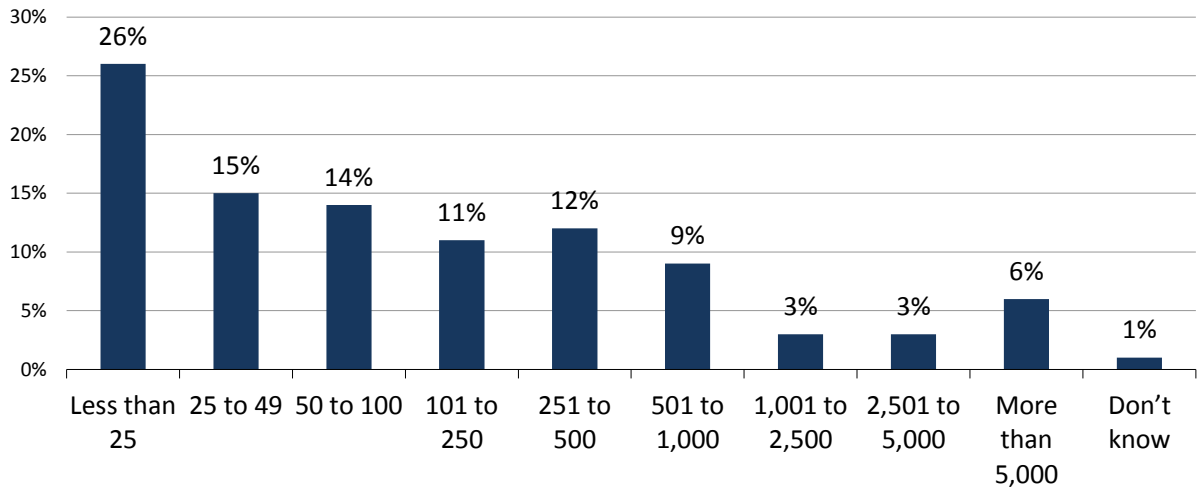


Source: Enterprise Strategy Group, 2013.

Respondents by Number of Physical Production Servers

The number of physical production servers (including both physical and virtual servers) supported worldwide in respondent organizations is shown in Figure 42.

Figure 42. Survey Respondents by Number of Physical Production Servers

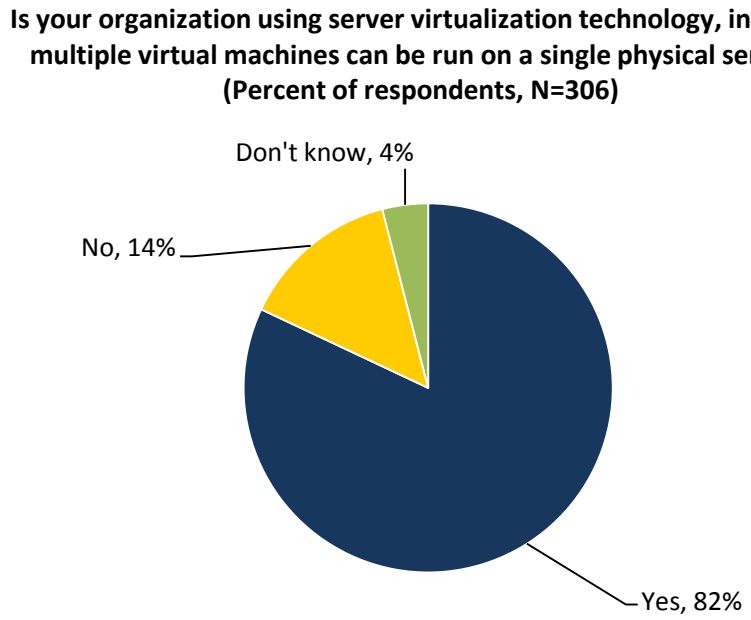


Source: Enterprise Strategy Group, 2013.

Respondents by Server Virtualization Usage

Respondent organizations' use of server virtualization technology is shown in Figure 43.

Figure 43. Survey Respondents by Server Virtualization Usage

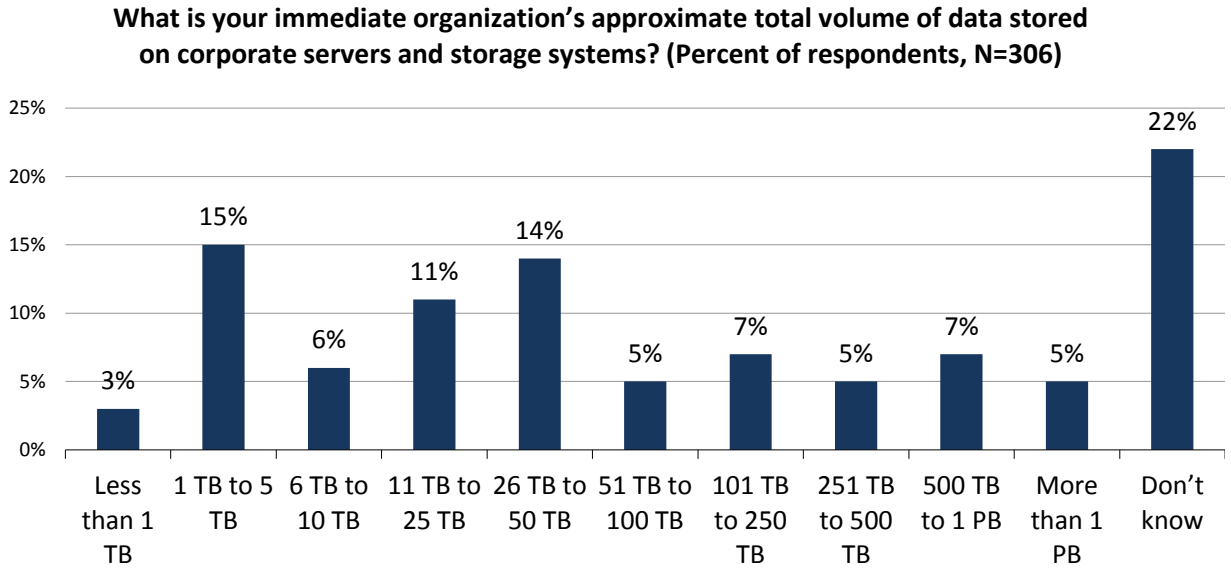


Source: Enterprise Strategy Group, 2013.

Respondents by Total Storage Capacity

Respondent organizations' total storage capacity is shown in Figure 44.

Figure 44. Survey Respondents by Total Storage Capacity

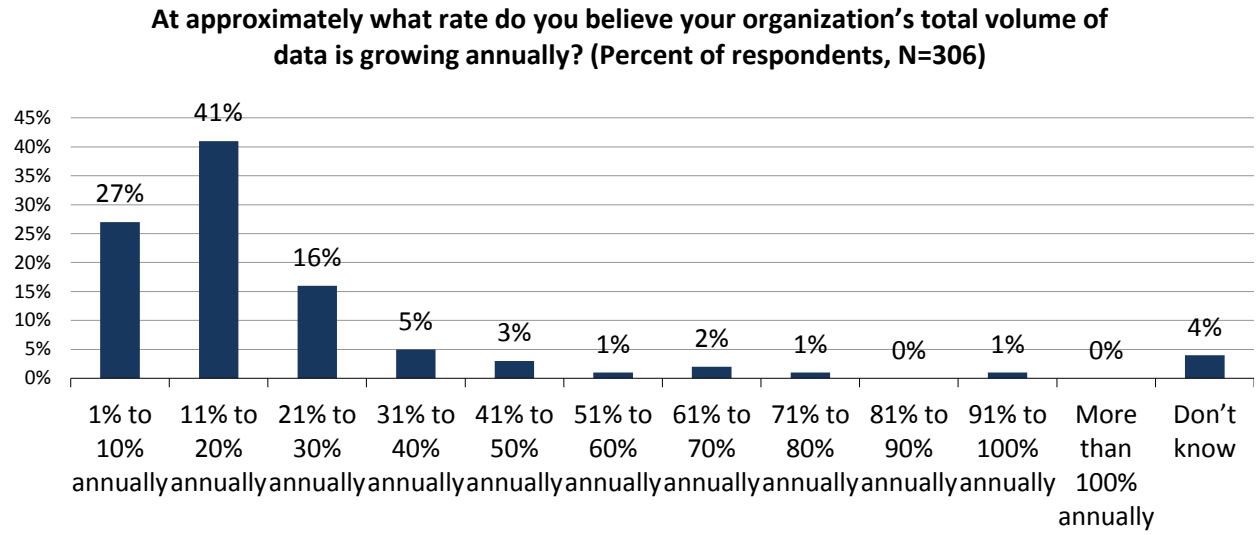


Source: Enterprise Strategy Group, 2013.

Respondents by Annual Data Growth Rate

The growth rate for total volume of data at respondent organizations is shown in Figure 45.

Figure 45. Survey Respondents by Annual Growth Rate

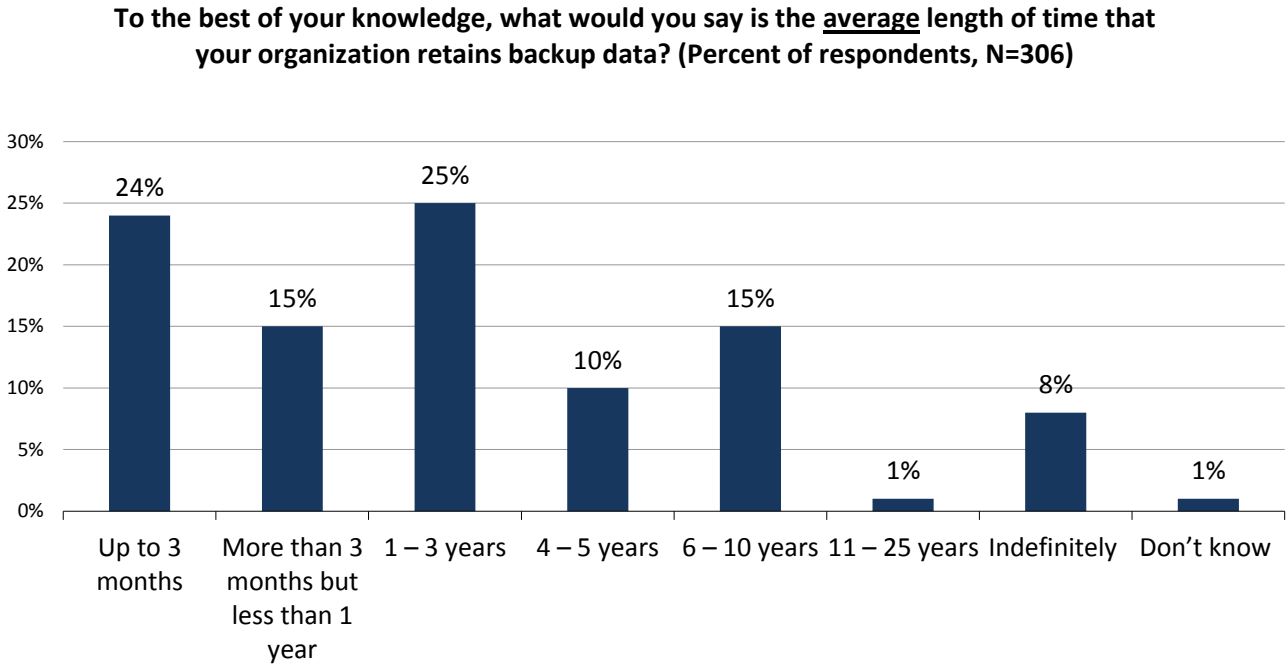


Source: Enterprise Strategy Group, 2013.

Respondents by Average Backup Data Retention Time

The average length of time respondent organizations retain backup data is shown in Figure 46.

Figure 46. Survey Respondents by Average Length of Time Backup Data Is Retained



Source: Enterprise Strategy Group, 2013.

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