Global Data Protection Index 2021

Key Findings – July 2021

VansonBourne

DELL Technologies

Focus of key findings

1. The data protection risk landscape
2. The threat posed by cyber attacks
3. Keeping pace with new and emerging technologies
4. Data protection vulnerabilities in cloud environments
5. The growth of as-a-Service
6. Simplifying data protection

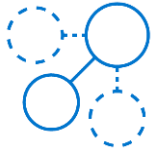
Five key takeaways

The widespread adoption of working from home has **increased data protection and cyber risks**

Many lack confidence in the capacity of their organization's data protection to sufficiently defend against and recover from cyber threats

Ongoing investments in emerging technologies and cloud **can add to data protection challenges**

Many are **interested in leveraging as-a-Service** to increase data protection simplicity and flexibility



There is evidence that working with **fewer data protection vendors** co-relates to **better data protection outcomes**

Who did we interview?

1,000 IT decision makers were interviewed in February, March and April 2021

Organizations from a wide range of public and private sector industries

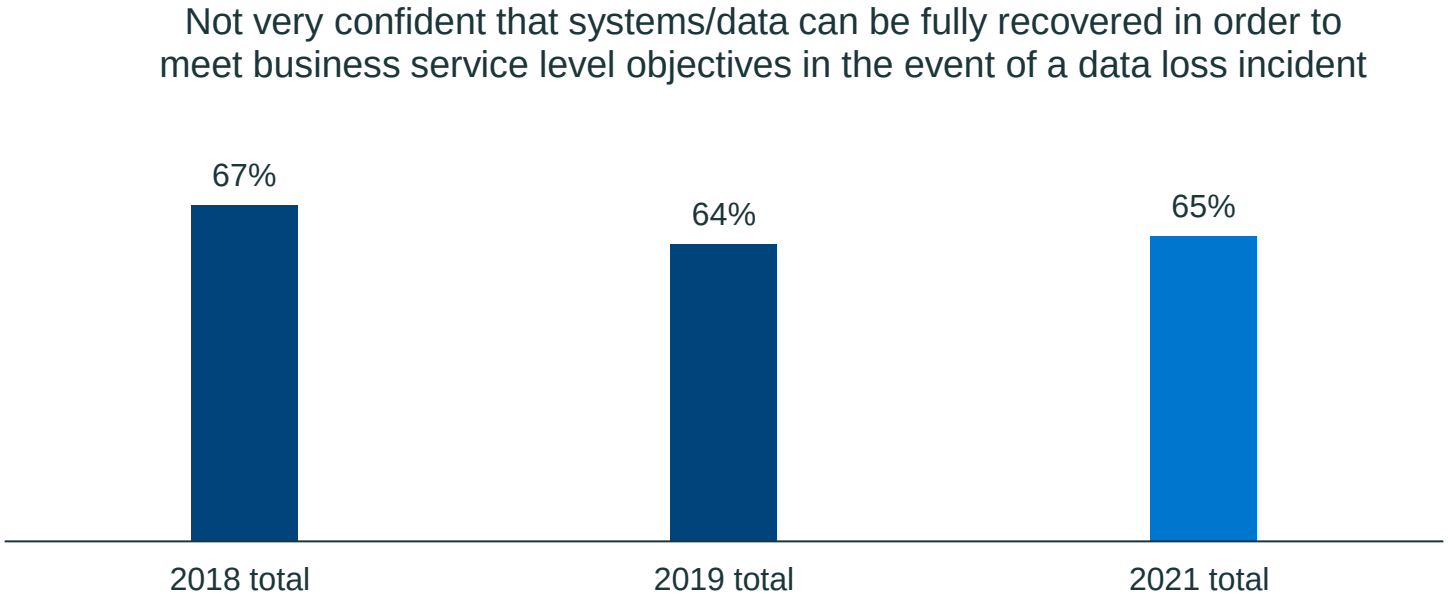
Organizations with 250+ employees

4 regions:

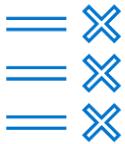
Americas (200)
EMEA (450)
APJ (250)
China (100)

1. The data protection risk landscape

IT decision makers lack confidence in their organization's ability to meet recovery SLOs



Further, confidence that data protection capabilities measure up to internal and external standards is low – this is made more concerning by the fact that two-thirds believe they will experience a disruptive event in the next year



58%

aren't very confident that their organization is **meeting its backup and recovery service level objectives**

63%

aren't very confident that their organization's current data protection infrastructure and processes are **compliant with regional data governance regulations**

64%

are **concerned that they will experience a disruptive event** in the next twelve months

Adding to this cause for concern is that the issues of data loss and systems downtime continue to have a significant financial impact on organizations

$959,493

average cost of data loss in the last 12 months (in USD)

$513,067

average cost of unplanned systems downtime in the last 12 months (in USD)

2. The threat posed by cyber attacks

Organizations lack confidence that their data protection measures can mitigate the effects of cyber attacks. Moreover most believe there is increased exposure with employees working from home

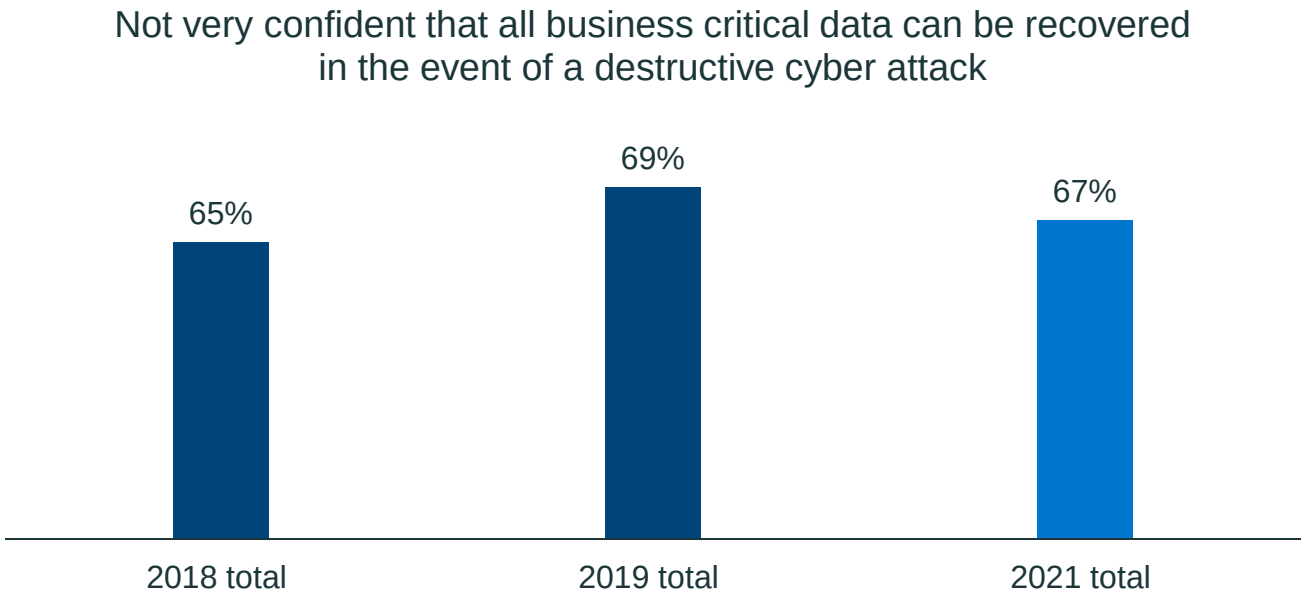
62%

are concerned their organization's existing data protection measures **may not be sufficient to cope with malware and ransomware threats**

74%

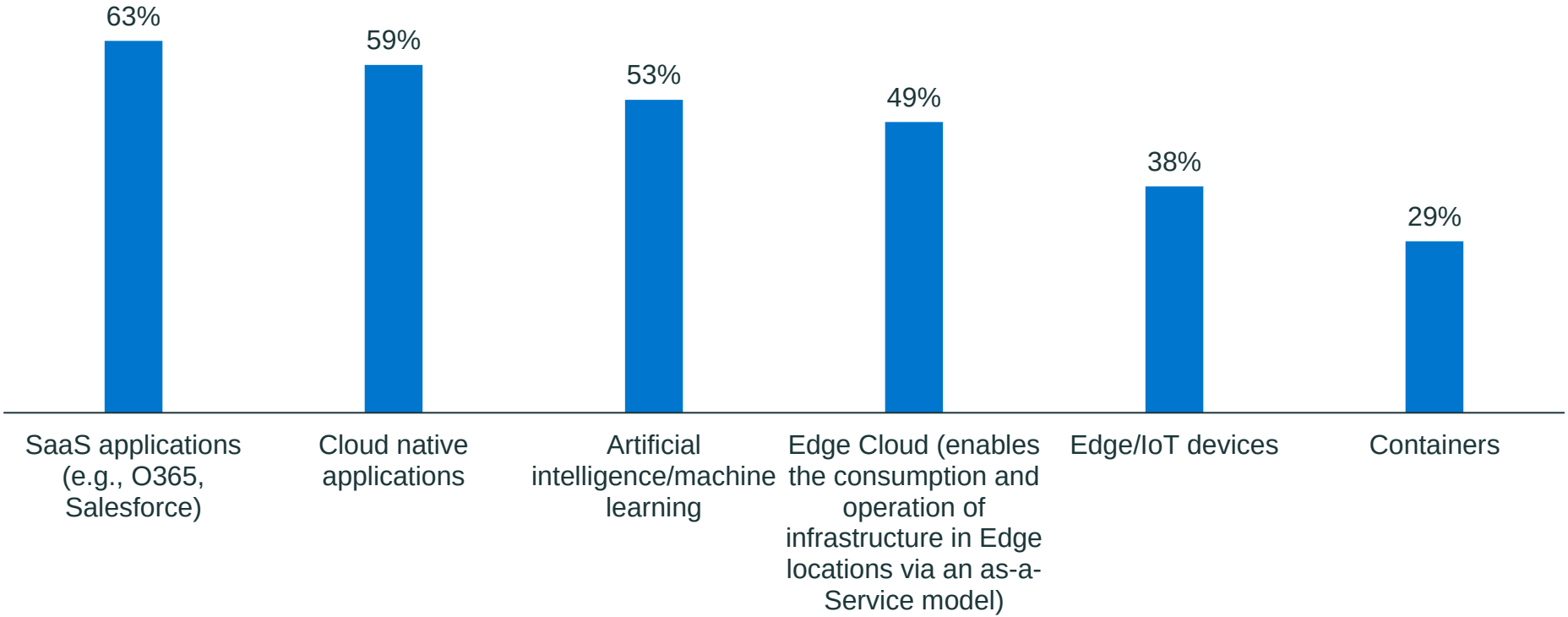
agree their organization has **increased exposure to data loss** from cyber threats with the growth of **employees working from home**

Compounding concern about organizations' ability to cope with malware and ransomware threats, many lack confidence that they would be able to recover all business critical data in the event of a destructive cyber attack

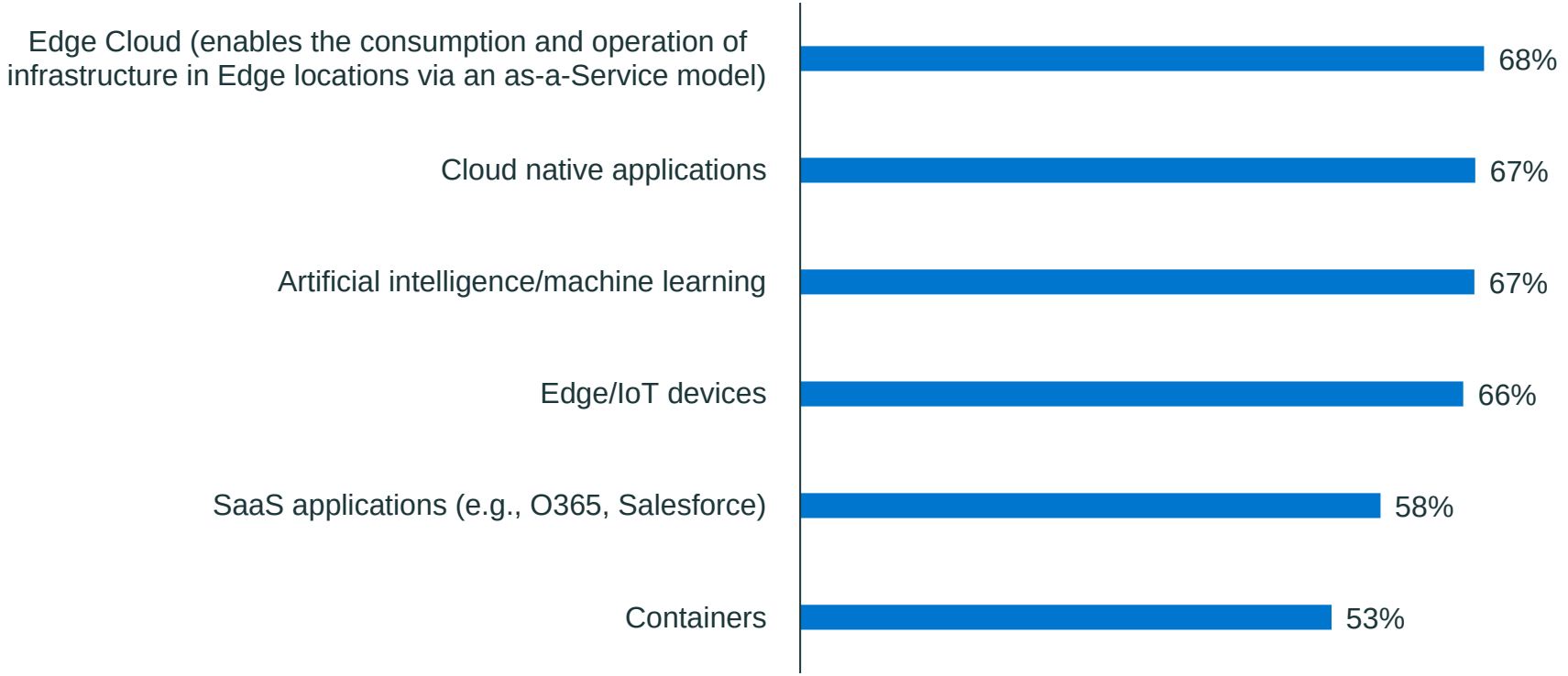


3. Keeping pace with new and emerging technologies

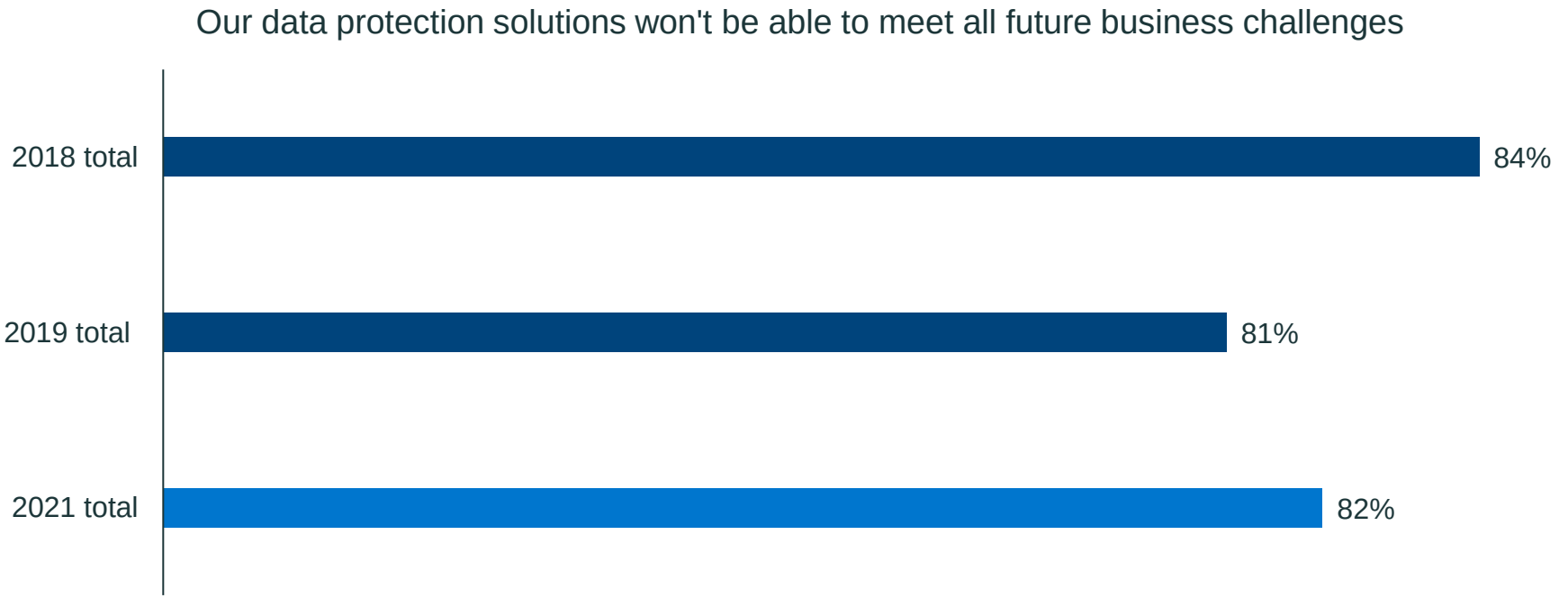
Organizations are investing in many new technologies, which could be complicating their data protection challenges



And it is the case that many organizations are struggling to protect these technologies



The difficulty of protecting new and emerging technologies is likely contributing to poor confidence that data protection solutions are future-ready



Many see emerging technologies as a data protection risk, and concern around future disruptive events is high, especially among those using multiple data protection vendors

Emerging technologies (such as AI, IoT, Edge) pose a risk to data protection

Use a single data protection vendor

57%

Uses multiple data protection vendors

64%

I am concerned that we will experience a disruptive event (e.g., data loss, systems downtime, etc.) in the next 12 months

Use a single data protection vendor

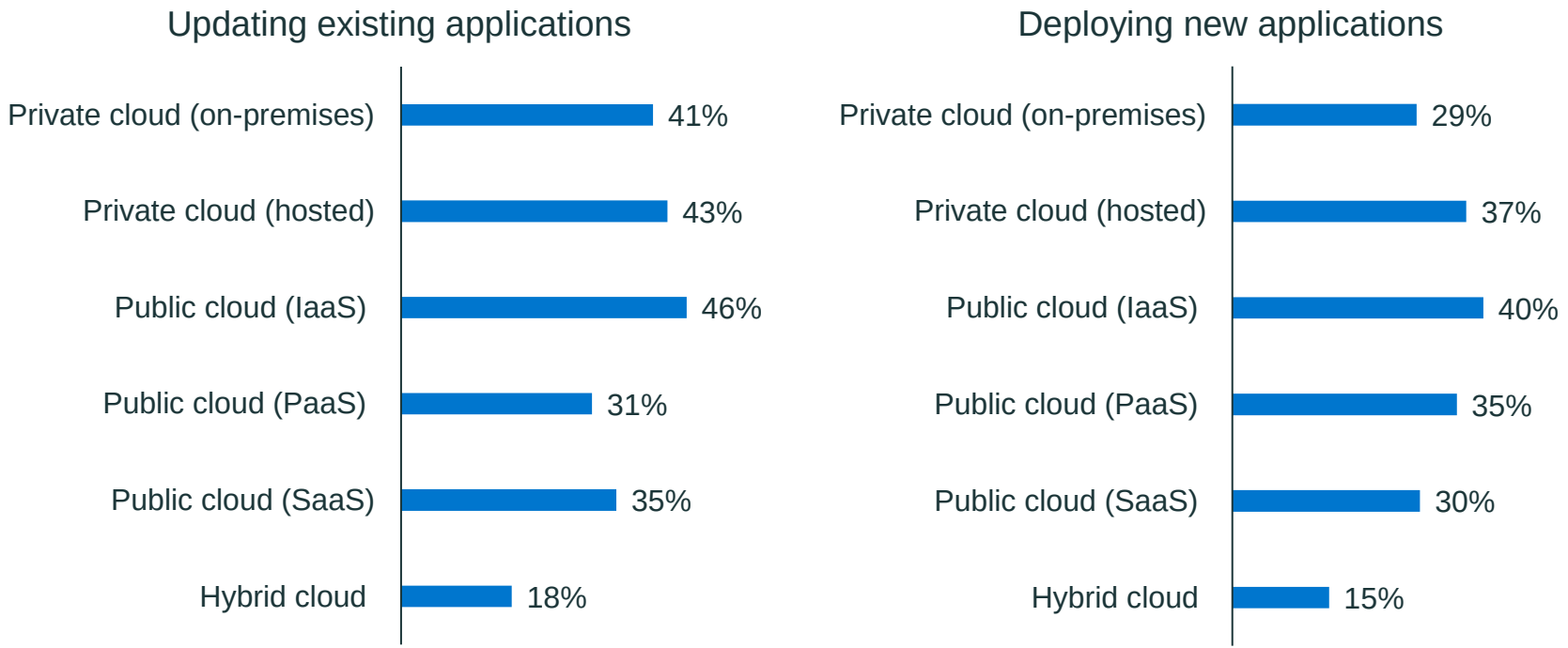
54%

Uses multiple data protection vendors

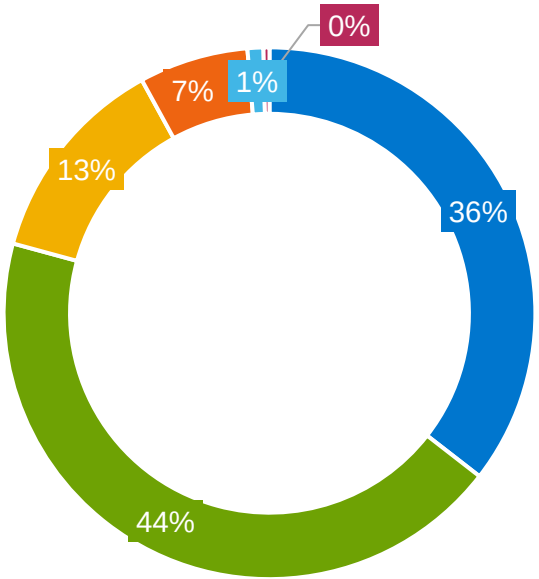
68%

4. Data protection vulnerabilities in cloud environments

Applications are being updated and deployed across a range of environments in organizations' IT infrastructures

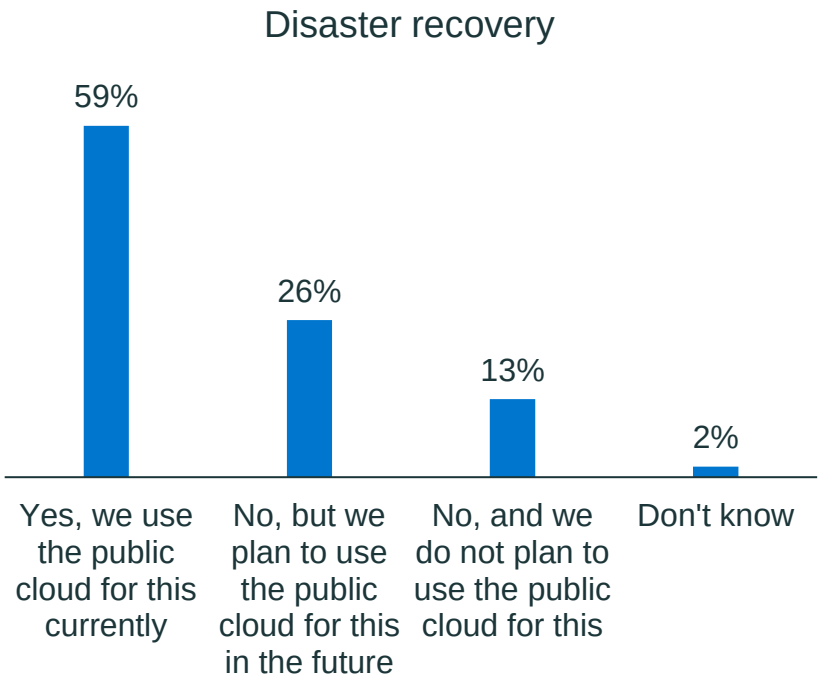


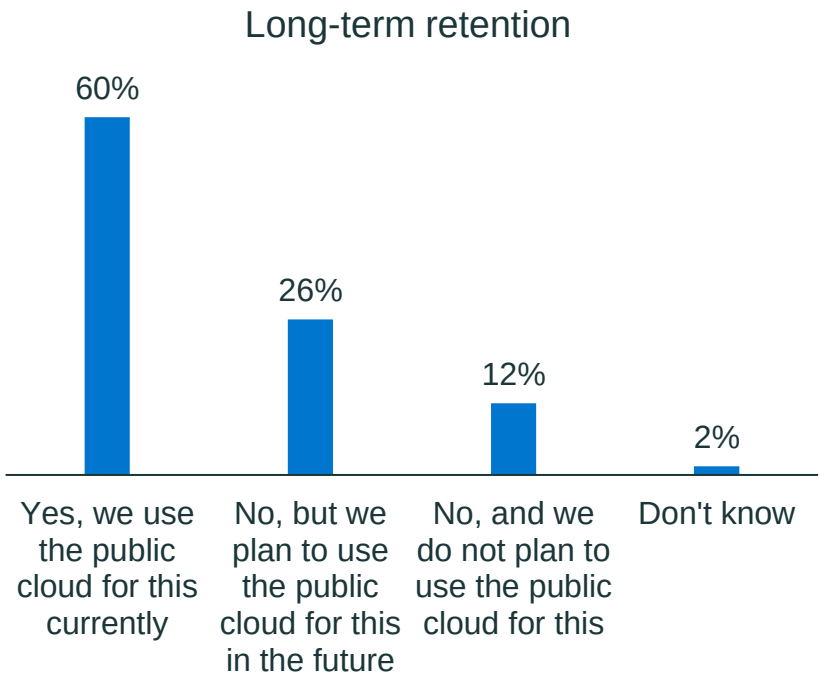
However, many are lacking confidence when it comes to how well they can protect their data across public cloud environments



- Very confident – we protect all of our data across public cloud
- Moderately confident – we protect all of our critical data across public cloud, but not all our total data
- Some doubt – we protect most of our critical data across public cloud
- Not very confident – we protect some of our critical data across public cloud
- Not at all confident – we do not protect our data across public cloud
- Don’t know

The public cloud has a growing role to play in organizations' disaster recovery and long-term retention strategies

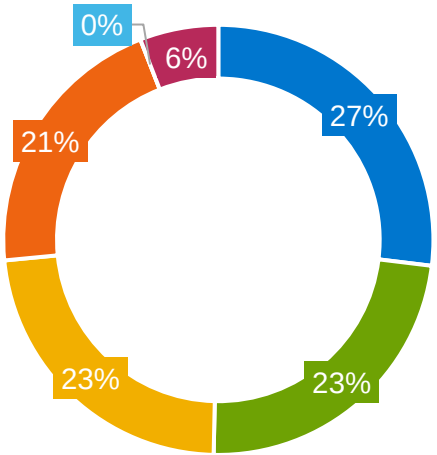




A number of organizations using multiple cloud environments aren't using specific solutions to protect them

21%

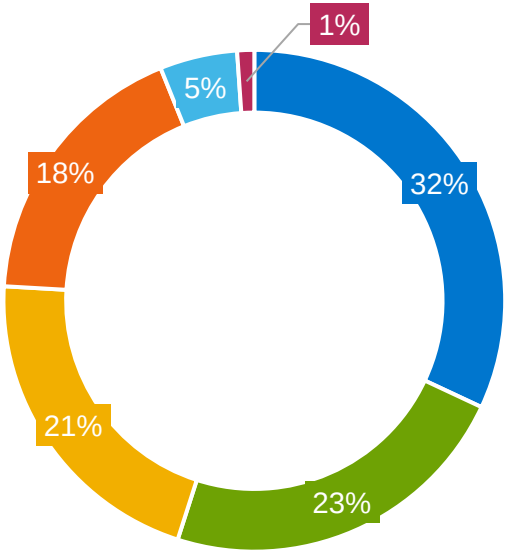
believe when using multiple cloud environments, **each cloud service provider** is responsible for **protecting their workloads**



- We plan to upgrade our data protection solution to enable the backup of workloads across multiple clouds
- Our current backup solution allows us to protect workloads running in multiple clouds
- We use multiple backup tools to protect workloads running in multiple clouds
- Each cloud service provider is responsible for protecting our workloads
- Other
- We are not running workloads in multiple cloud environments

And similar is true when considering the protection of virtualized workloads using VMware in the cloud

- We plan to upgrade our data protection solution to enable hybrid cloud backup of VMware workloads
- Our cloud service provider is responsible for protecting our workloads
- With backup tools that we currently use and operate on-premises
- With backup tools available in the cloud service provider marketplace
- We are not running or planning to run virtualized workloads using VMware in the cloud
- Don't know

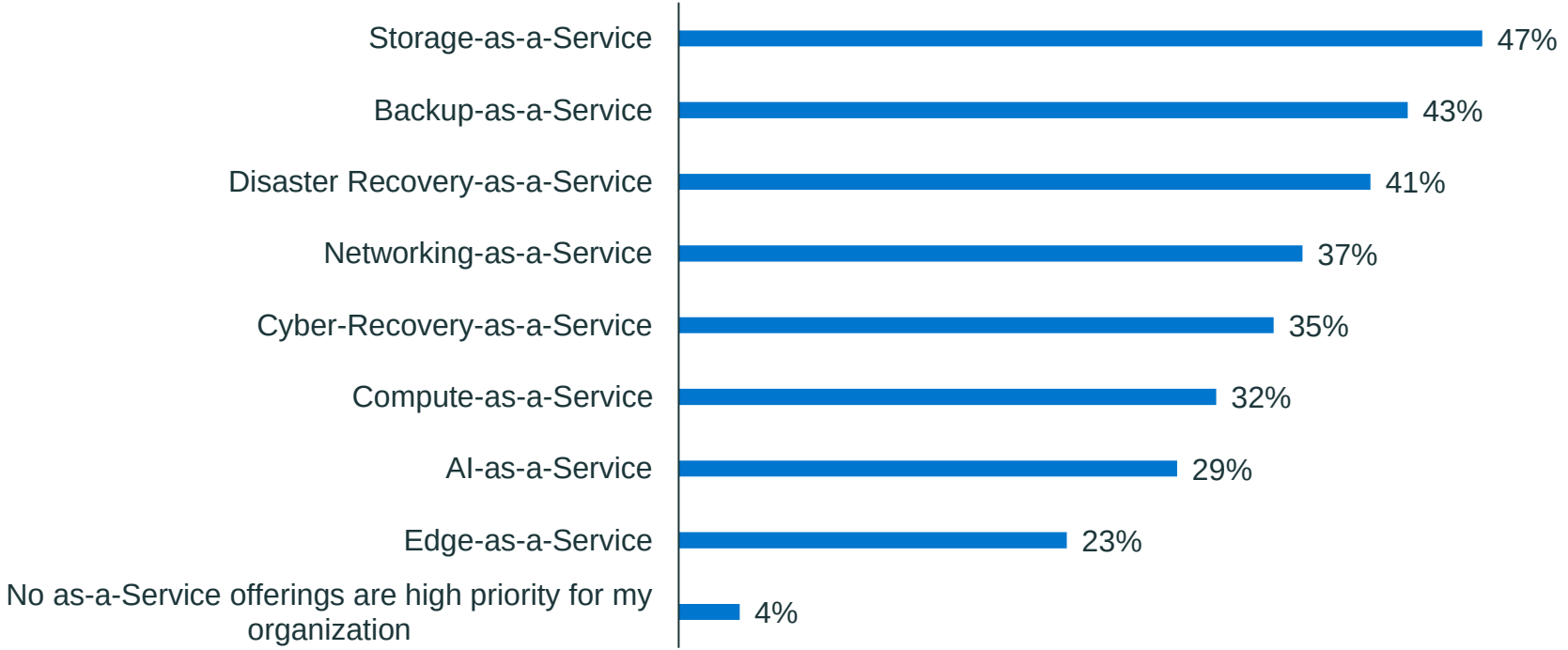


23%

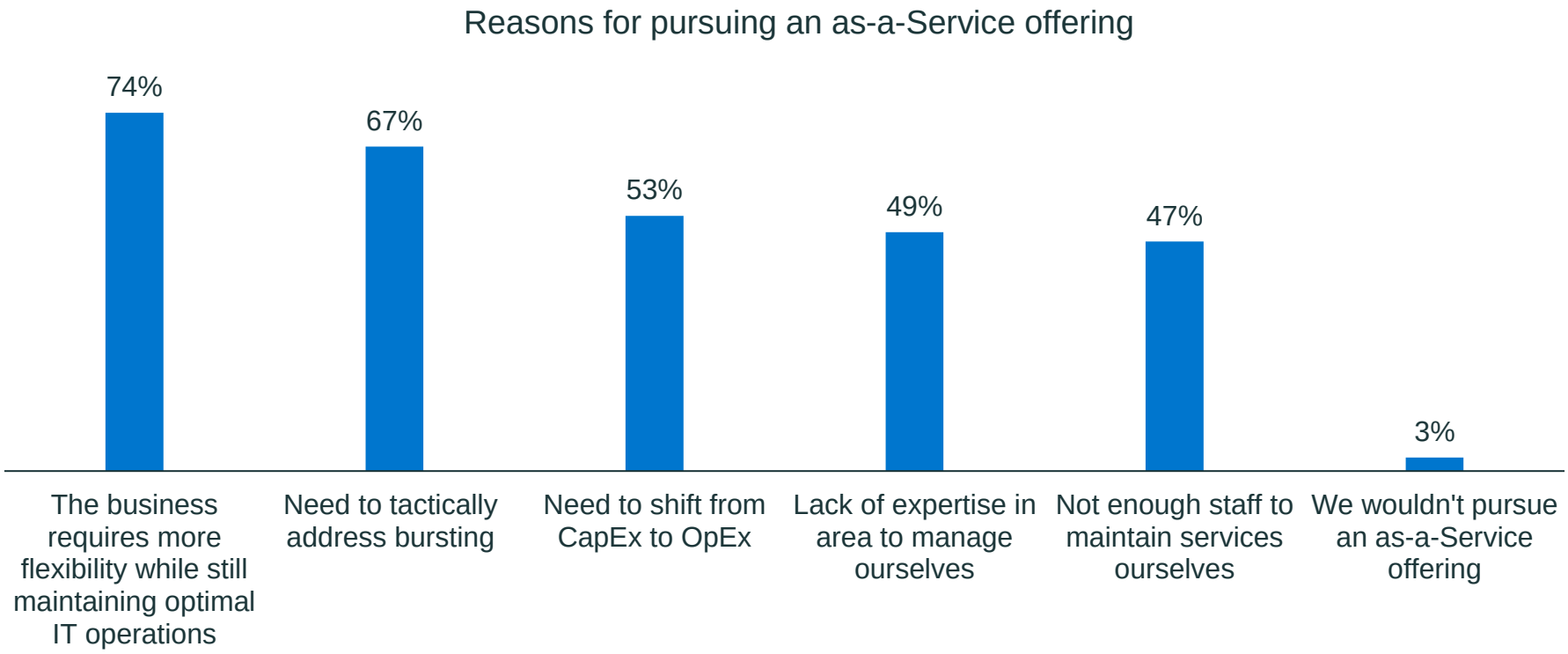
believe their **cloud service provider** is responsible for **protecting their virtualized workloads**

5.The growth of as-a-Service

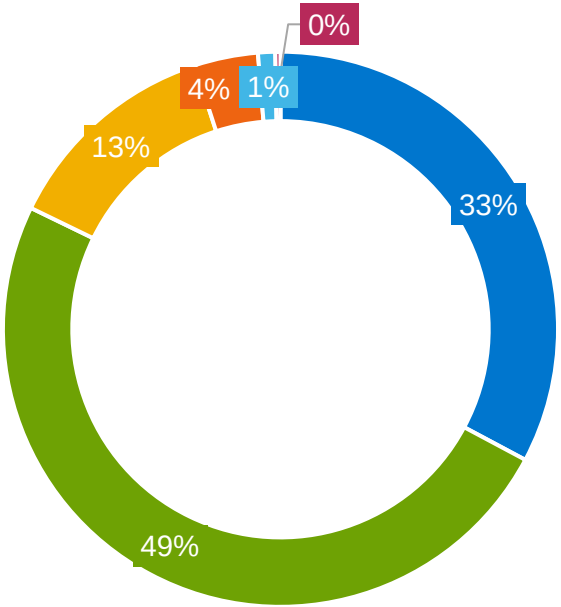
As-a-Service offerings are being prioritized by most organizations, with Backup-as-a-Service and Disaster Recovery-as-a-Service among the most commonly prioritized



The popularity of as-a-Service offerings often stems from their flexibility



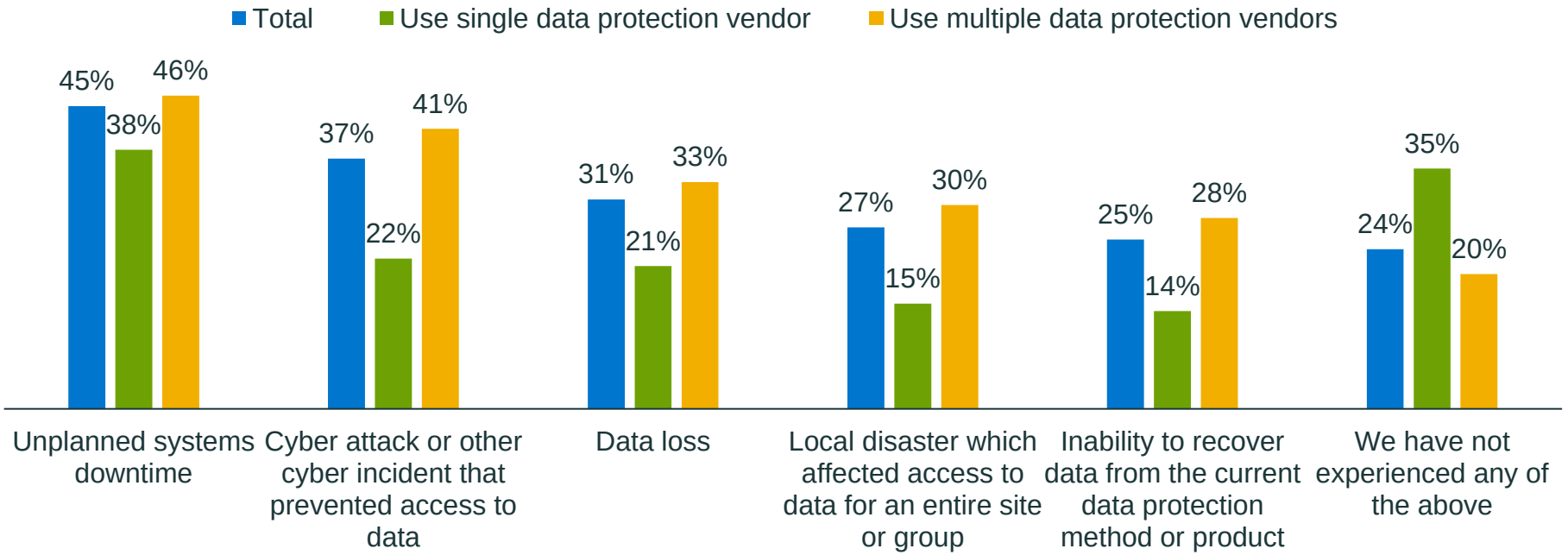
The vast majority would prefer to work with a vendor which has multiple as-a-Service offerings, suggesting a desire to consolidate their workloads with fewer vendors



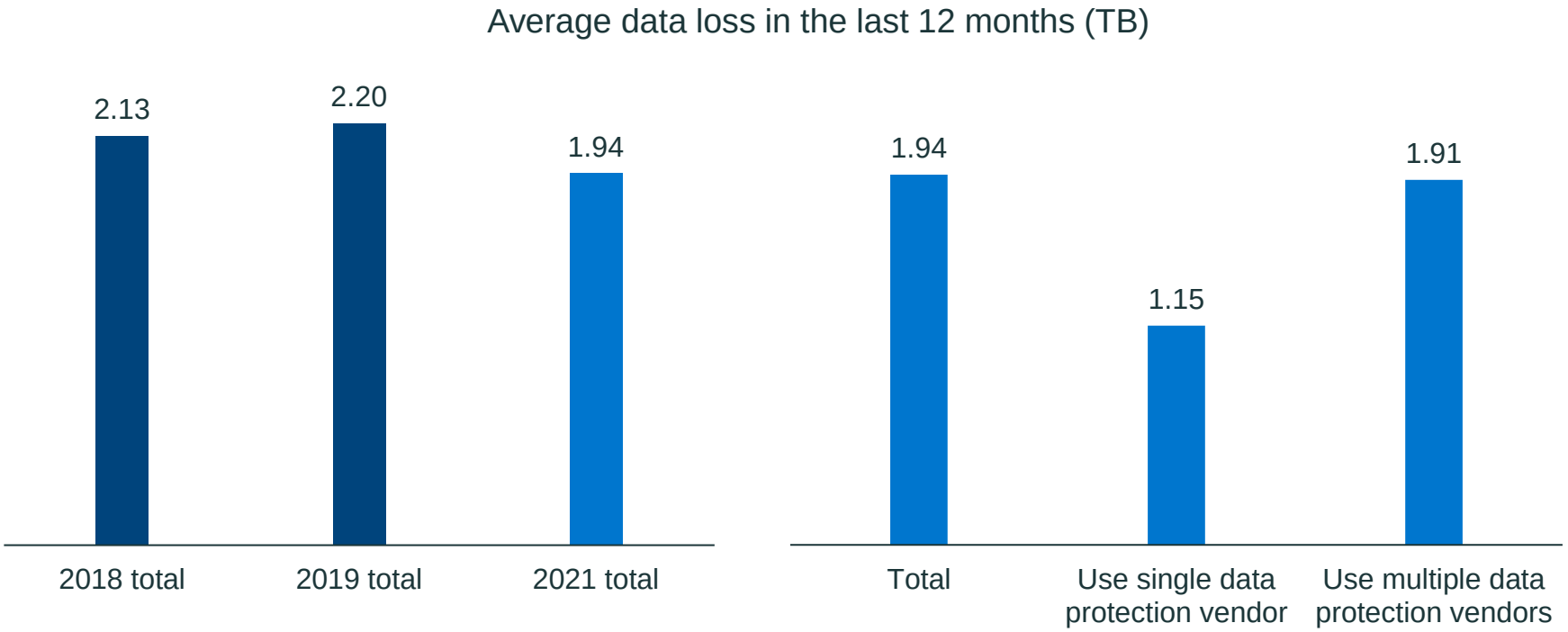
- We are far more likely to pursue a vendor which has multiple as-a-Service offerings
- We are slightly more likely to pursue a vendor which has multiple as-a-Service offerings
- I am indifferent as to whether a vendor has multiple as-a-Service offerings
- We are slightly less likely to pursue a vendor which has multiple as-a-Service offerings
- We are far less likely to pursue a vendor which has multiple as-a-Service offerings
- Don’t know

6. Simplifying data protection

Organizations using multiple data protection vendors are more likely to have suffered from many issues relating to data loss, data access or systems downtime in the past year than those using only a single vendor



And organizations which are using multiple data protection vendors are losing more data, on average, than those using a single vendor



Key findings – in summary (1/2)

The data protection risk landscape

- Many have concerns that they wouldn't be able to recover all systems/data to meet SLOs in the event of a data loss incident
- Fear is widespread that organizations will experience a disruptive event in the next twelve months and the impacts of these disruptive events could be financially devastating
- Organizations must take action to ensure they are prepared to respond to these events if they occur

The threat posed by cyber attacks

- Concern is high that organizations aren't able to protect against malware and ransomware threats and most agree that the risk of cyber attacks has increased with the growth of remote work
- If organizations are to suffer attacks, few are confident their organization would be able to recover all business critical data

Keeping pace with new and emerging technologies

- Organizations are investing in a range of new and emerging technologies, including SaaS applications, AI/ML and Edge/IoT devices, but often struggling to ensure that their data protection keeps up
- Many believe that these technologies pose a risk to data protection and these risks are likely contributing to fears that organizations aren't future-ready, and that they are at risk of disruption in the next twelve months
- Investments in emerging technology is a good thing and should be encouraged, but organizations must ensure that their data protection infrastructure supports these technologies

Key findings – in summary (2/2)

Data protection vulnerabilities in cloud environments

- Applications are being updated and deployed across a range of cloud environments, yet confidence is often lacking when it comes to how well data can be protected
- The cloud plays an important role in disaster recovery and long-term retention strategies
- Organizations need to ensure they have specific solutions in place to protect data in multi-cloud and virtualized workloads, as some organizations still believe their cloud providers are responsible for this

The growth of as-a-Service

- As-a-Service solutions are of interest to most organizations, and will likely form a part of many organizations' data protection solutions going forwards – flexibility is often a key reason for this interest
- The preference for most would be to use as-a-Service solutions from vendors with multiple offerings, a choice which could help to simplify data protection for these organizations

Simplifying data protection

- Organizations which are using a single data protection vendor are less likely to have experienced data loss, data access issues and unplanned systems downtime incidents in the past year than those using multiple vendors
- Those using a single vendor have also lost less data than those using multiple solutions, on average
- While organizations may be tempted to expand their data protection capabilities by investing in new solutions, by consolidating their solutions with one vendor they are likely to be better protected against data loss and downtime

Mitigate risk and get ahead of the curve

Dell Technologies point of view

Conduct regular data protection readiness reviews

Make cyber resiliency a top priority

Consolidate data protection initiatives with Dell

Go to DellTechnologies.com/GDPI to learn more


DELL Technologies