Global Data Protection Index 2022

Key Findings – October 2022

VansonBourne

DELL Technologies

Focus of key findings

1
The data protection risk landscape

2
The increasing threat posed by cyberattacks

3
Protecting new and emerging tech

4
Securing a cloud environment

5
Looking to the future: the growth of as-a-Service

6
Simplifying data protection

Five key takeaways

The last 12 months have brought **higher levels of disruption** for organizations than in previous years

Experience of **cyberattacks or incidents** are more prevalent this year and are **contributing** to increased disruption

Almost all are **facing challenges** in relation to **data protection**

There has been a shift towards **public cloud use**, which may create **further data protection** issues for organizations

Working with **fewer data protection vendors** is linked to **better data protection outcomes**

Who did we interview?

1,000 IT decision makers were interviewed in August, September and October 2022

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

Concerns and a lack of confidence surrounding the capabilities of their existing data protection measures are prevalent, exposing organizations to risk

55%

are **not very confident** that their organization is **meeting its backup and recovery service level objectives (SLOs)**

69%

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

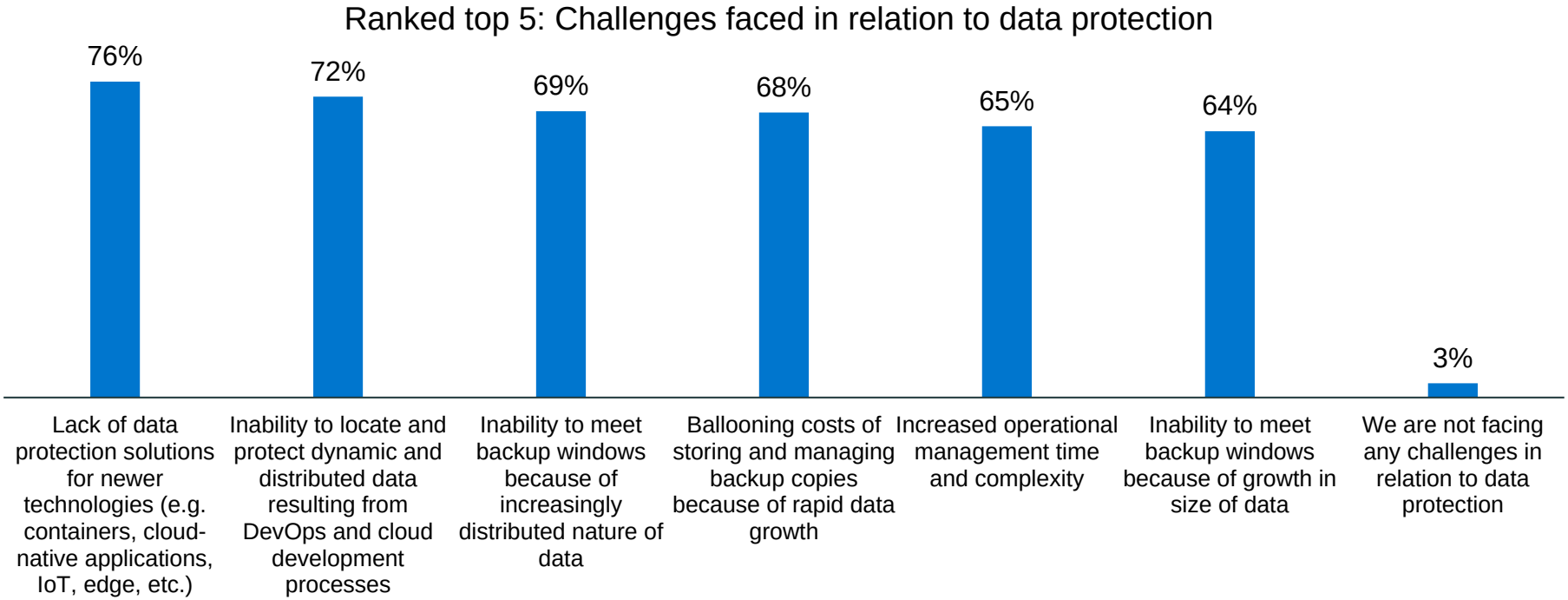
67%

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

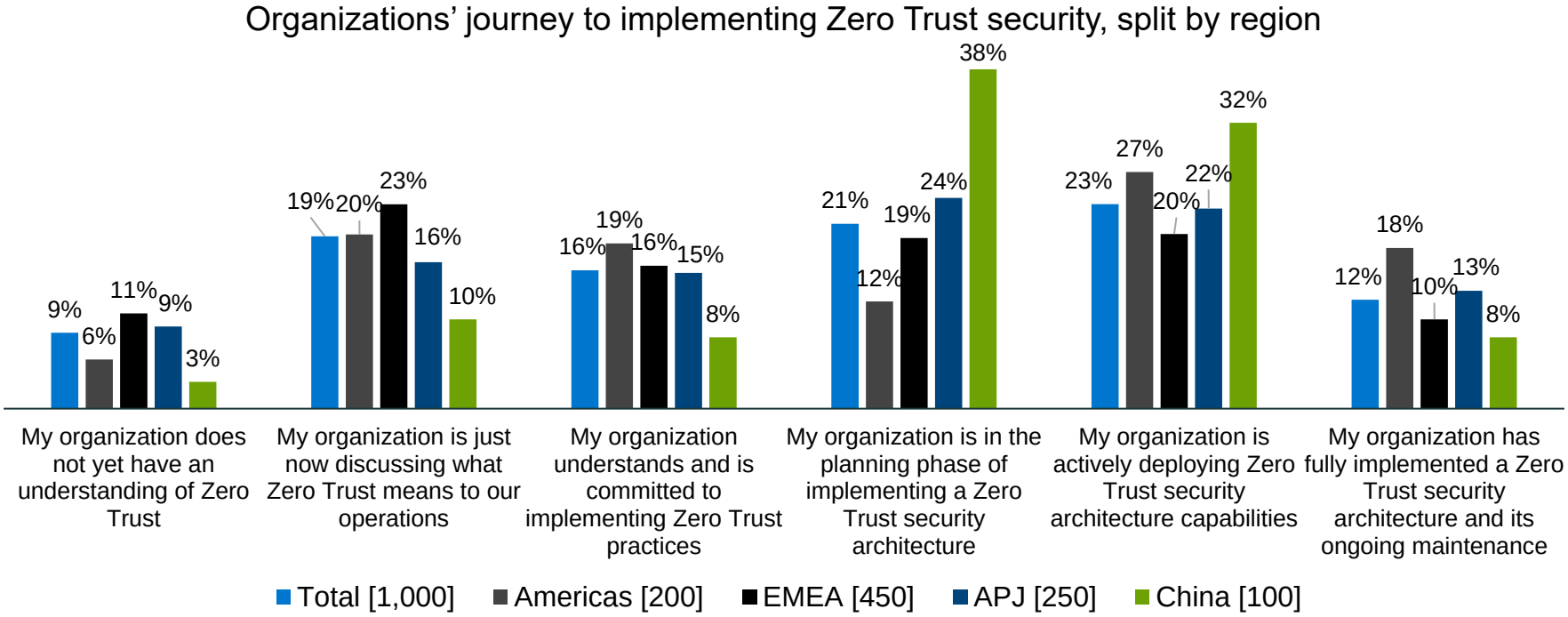
70%

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

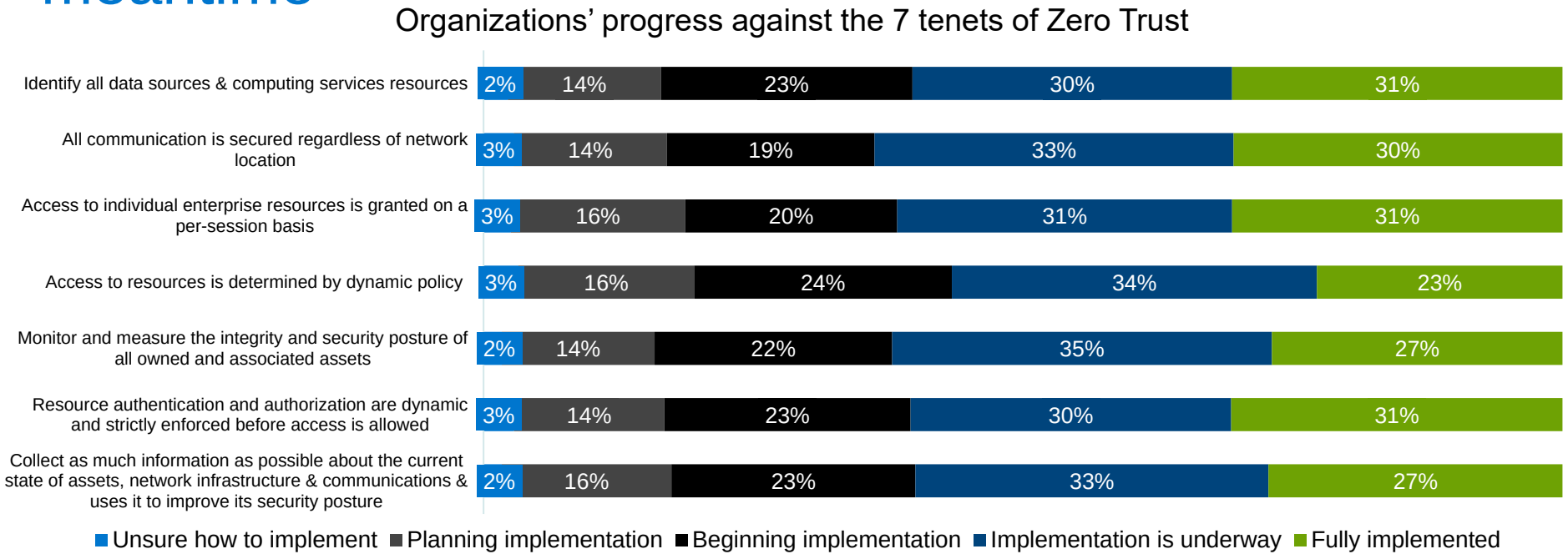
Alongside commonplace data protection challenges organizations are faced with



Although many organizations have an understanding and are planning or deploying Zero Trust security, few have fully implemented the architecture

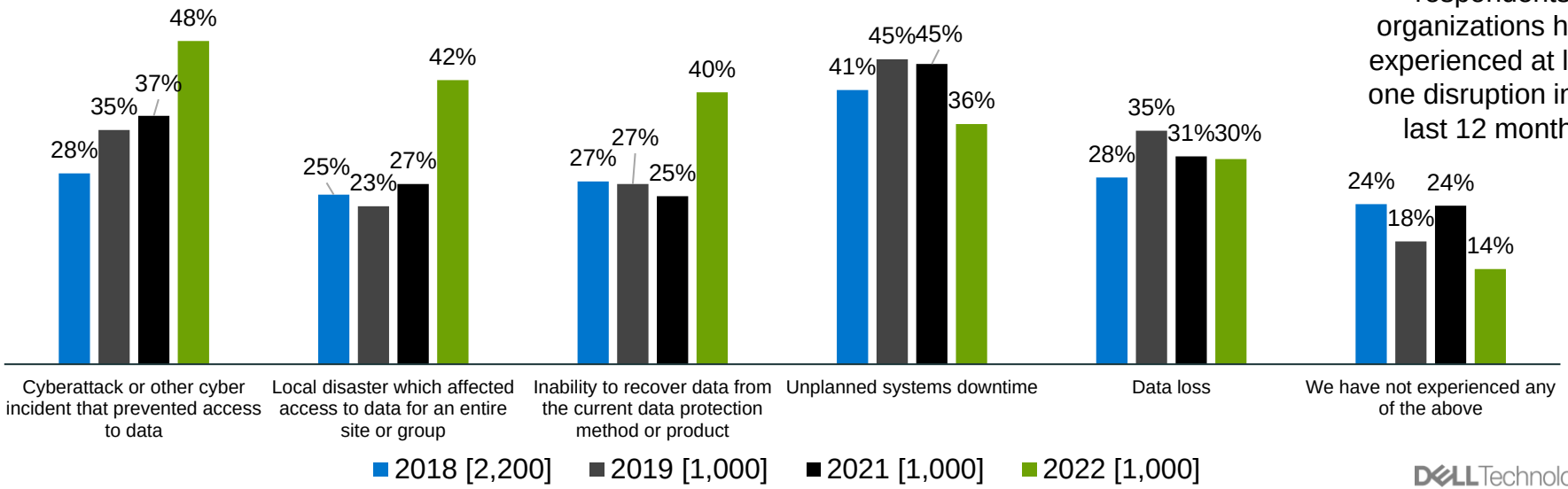


The majority of organizations still have a way to go to ensure Zero Trust is executed to best-practice standards and are potentially vulnerable to risk in the meantime



In addition, levels of disruption which are more likely being driven by cyber incidents, local disasters and problems recovering from current data protection methods have increased…

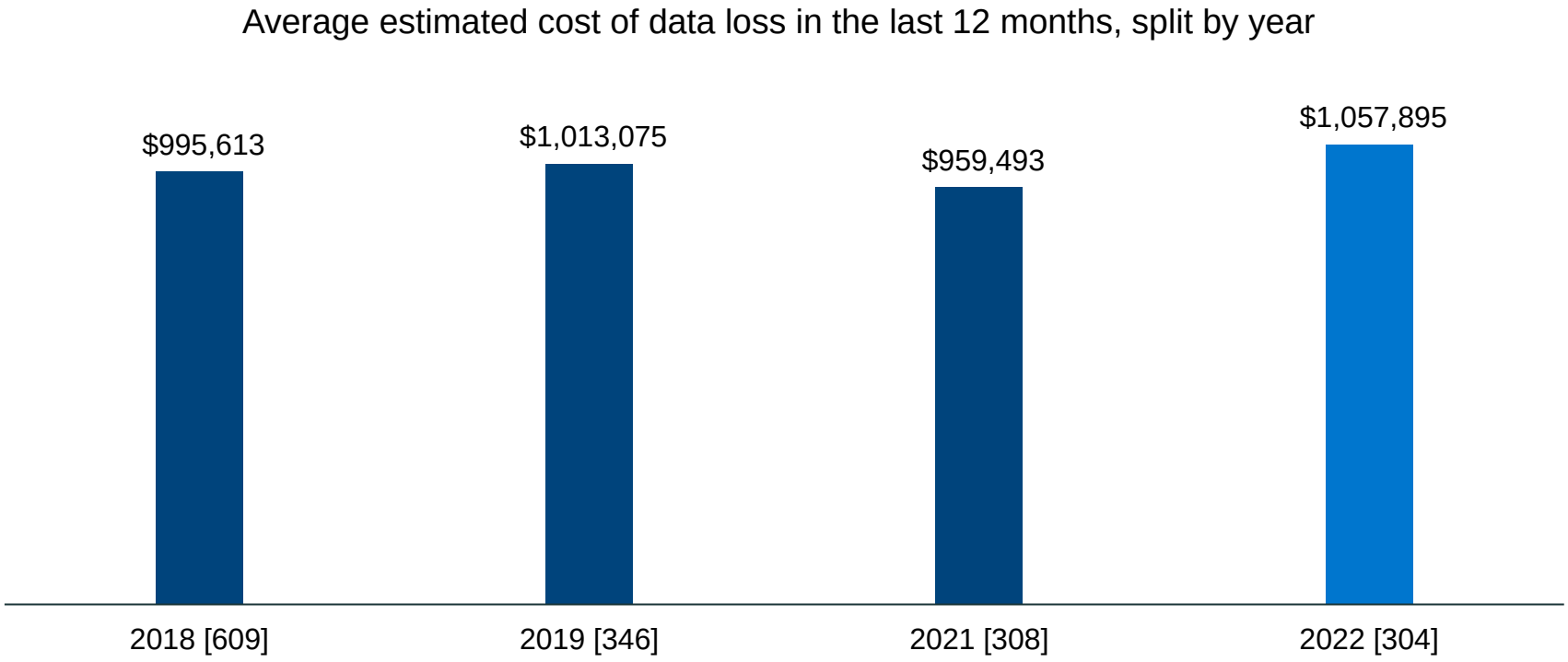
Organizations suffering various disruptions in the last 12 months, split by year



86%

…of 2022 respondents' organizations have experienced at least one disruption in the last 12 months

…with data loss increasingly impacting bottom lines



2. The increasing threat posed by cyberattacks

Confidence that organizations' data protection measures can mitigate the effects of cyberattacks is lacking. Moreover, most are aware there are increased vulnerabilities with employees working from home

67%

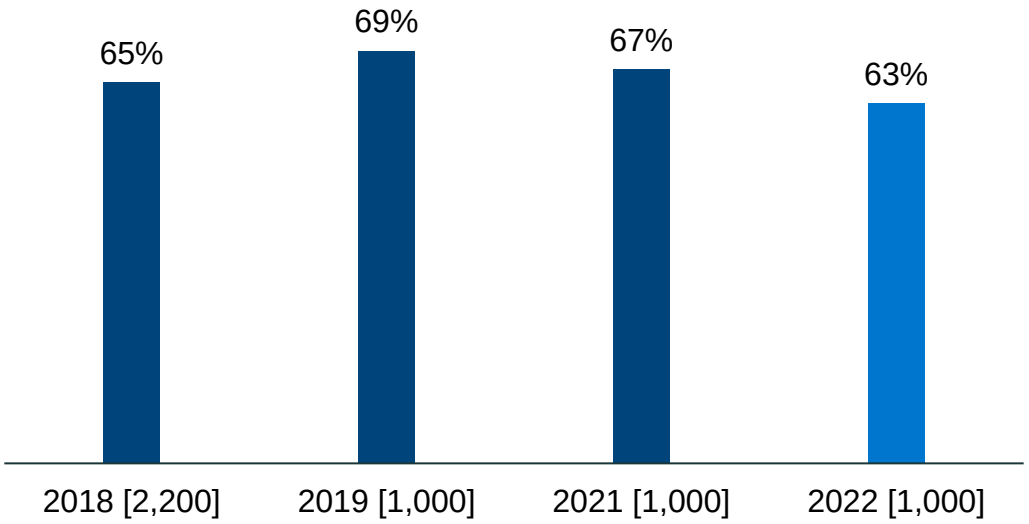
are concerned their organization's existing data protection measures **may not be sufficient to cope with malware and ransomware threats**

70%

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

This lack of confidence is echoed in their organization's ability to recover business-critical data in the event of cyberattack

Not "very confident" that all business-critical data can be reliably recovered in the event of a destructive cyberattack, split by year



Compounding this, there is a misguided over-confidence surrounding the consequences of a ransomware attack, another factor that could expose organizations to further risk

64%

…agree that their job and the employees within their organization **will not be affected by a ransomware attack**

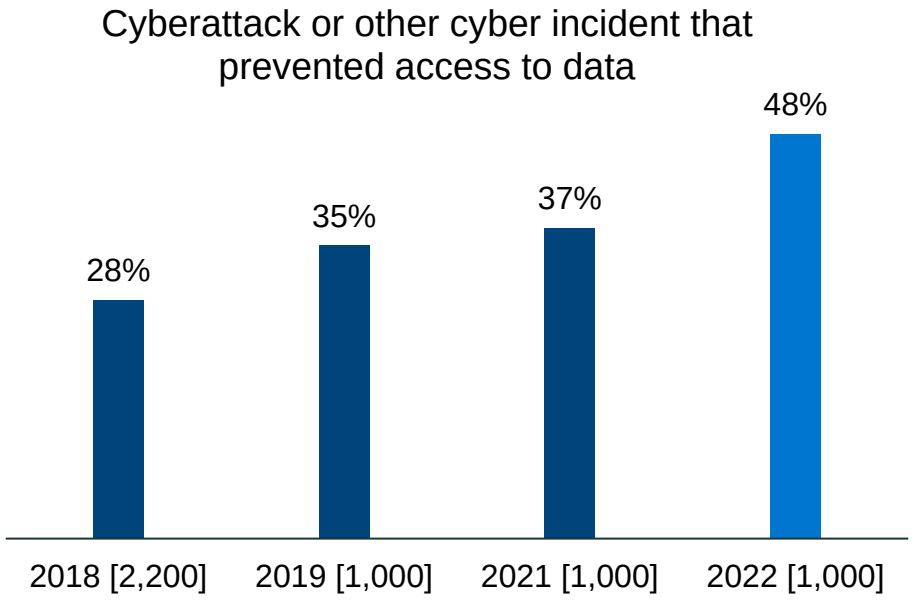
61%

…agree that if their organization suffers a ransomware attack, they'll **get all data back** to resume business **if they pay the ransom**

54%

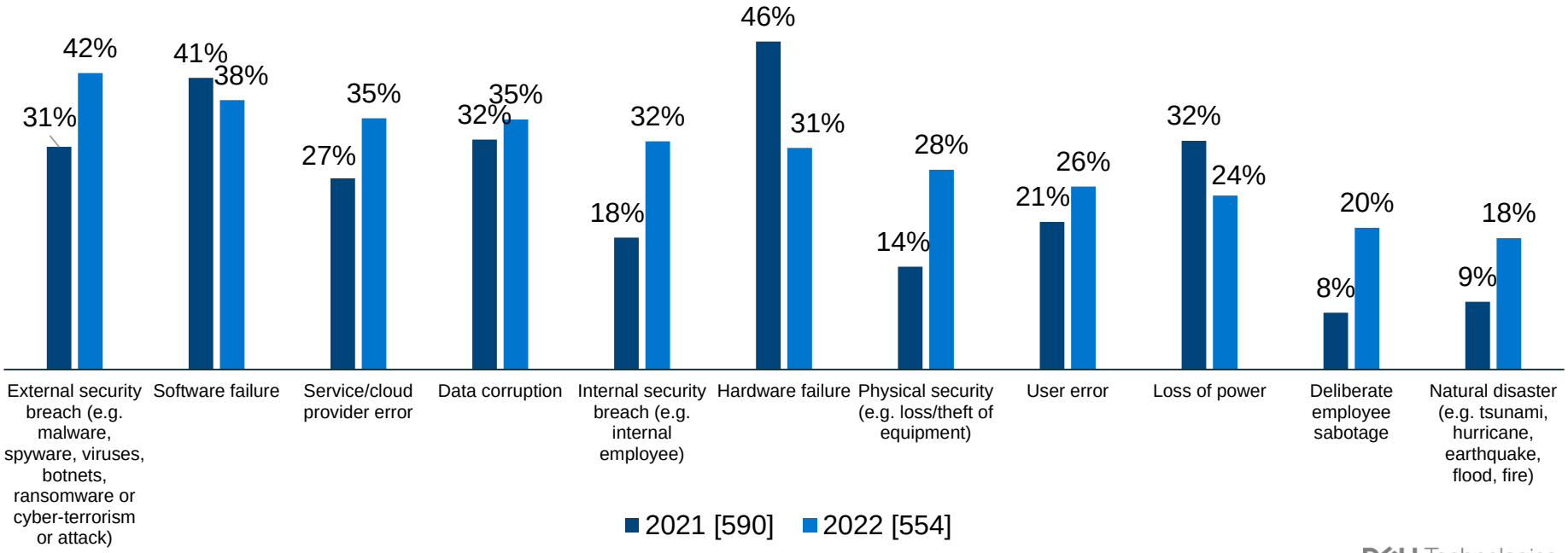
…agree that if their organization suffers a ransomware attack, once they pay the ransom **they won't be attacked again**

Which is concerning as there has been a considerable increase in IT decision makers reporting that their organizations' have suffered a cyberattack or other cyber incident in the last 12 months

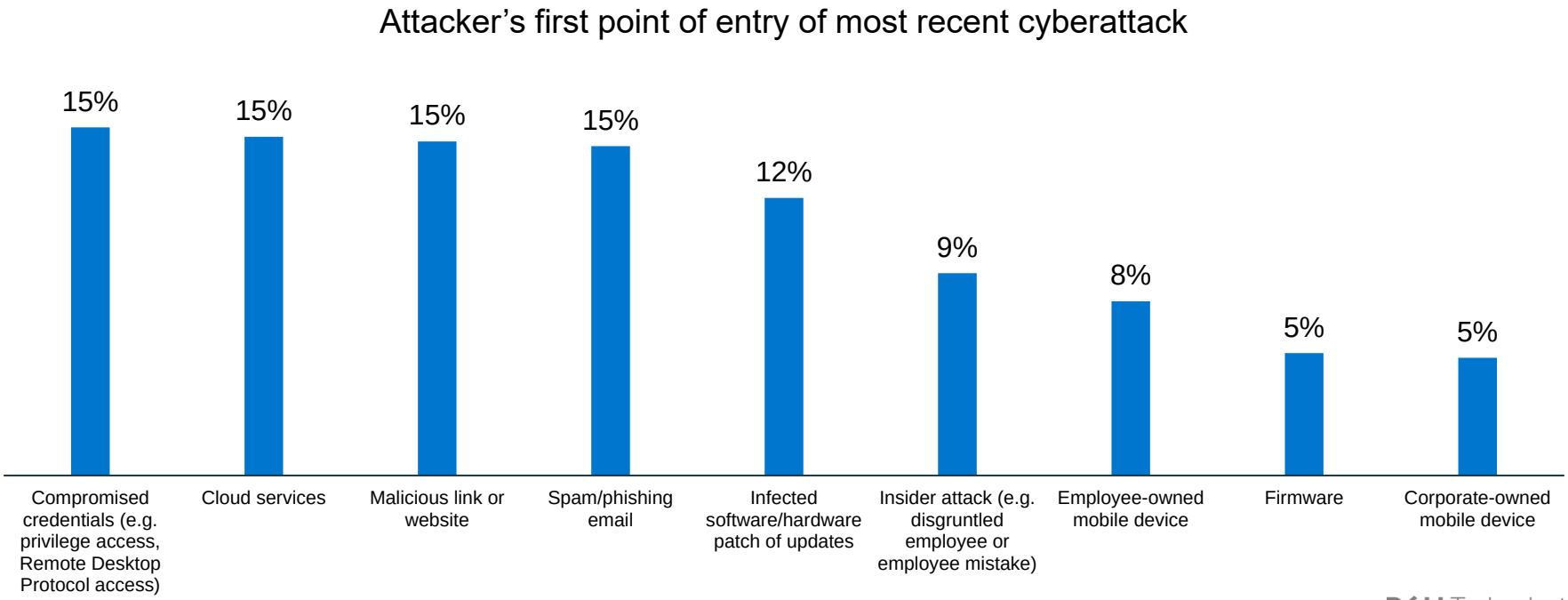


Even those who suffered data loss and/or systems downtime are more likely to cite security breaches as their cause, considerably increasing since 2021

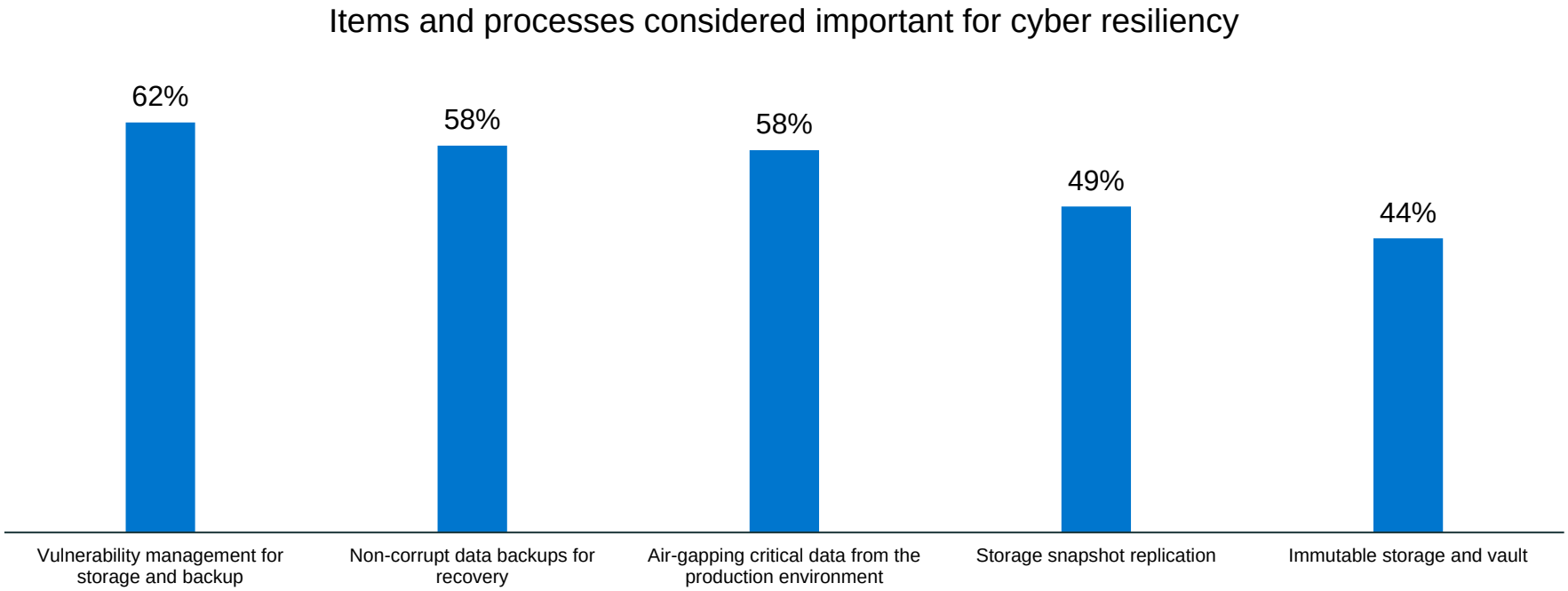
Causes of data loss and/or systems downtime, split by year



When they do attack, cyberattackers reportedly use various points of entry, with external attacks more likely compared to internal ones



There is some variation in what organizations consider important for cyber resiliency



3. Protecting new and emerging tech

Adopting newer technology can help drive modernization, but many report a lack of data protection solutions for them as a challenge and barrier

49%

report that **protecting newer workloads** such as containers, SaaS, and cloud-native apps (MongoDB, PostgreSQL, Cassandra, etc.) are a **barrier to their organizations' digital transformation/application modernization initiatives**

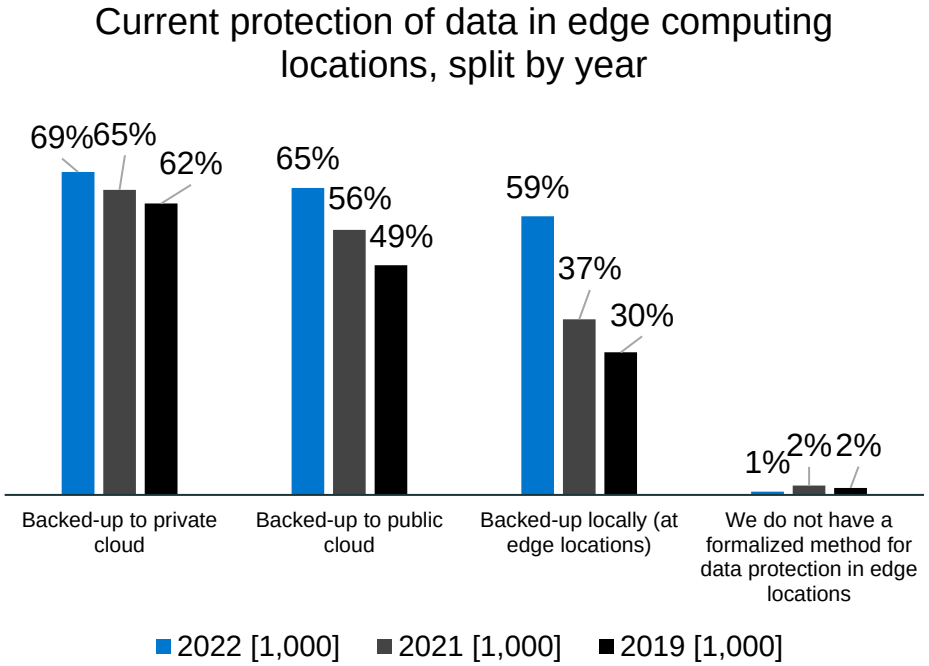
76%

rank a **lack of data protection solutions for newer technologies** (e.g. containers, cloud-native applications, IoT, edge, etc.) within **the top 5 challenges** their organization faces in relation to data protection

Many see emerging technologies posing a risk to data protection and, potentially as a result, are increasing security in edge computing locations

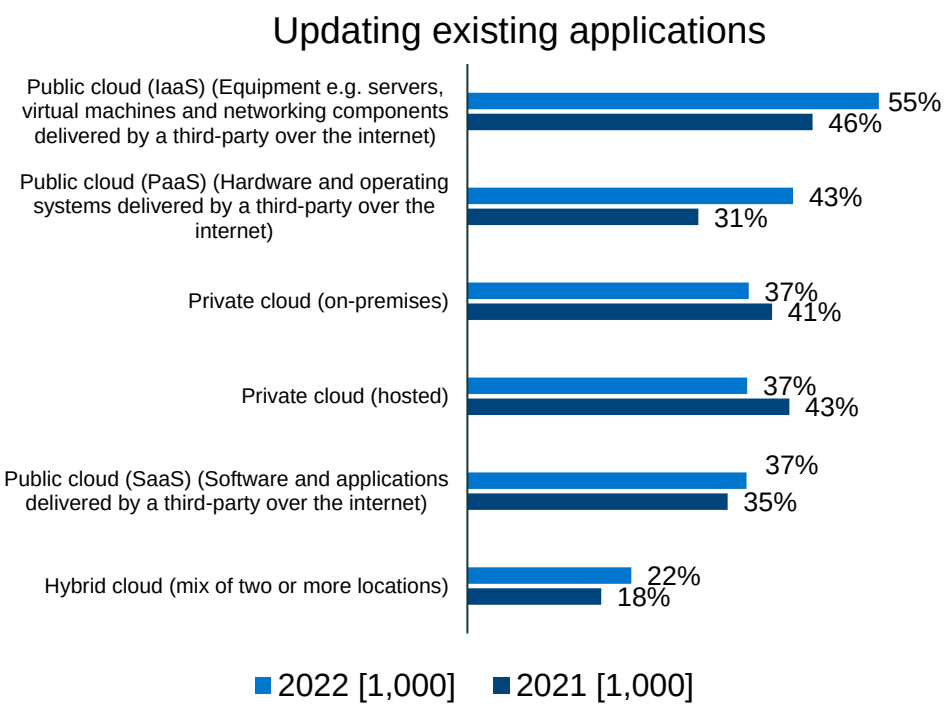
67%

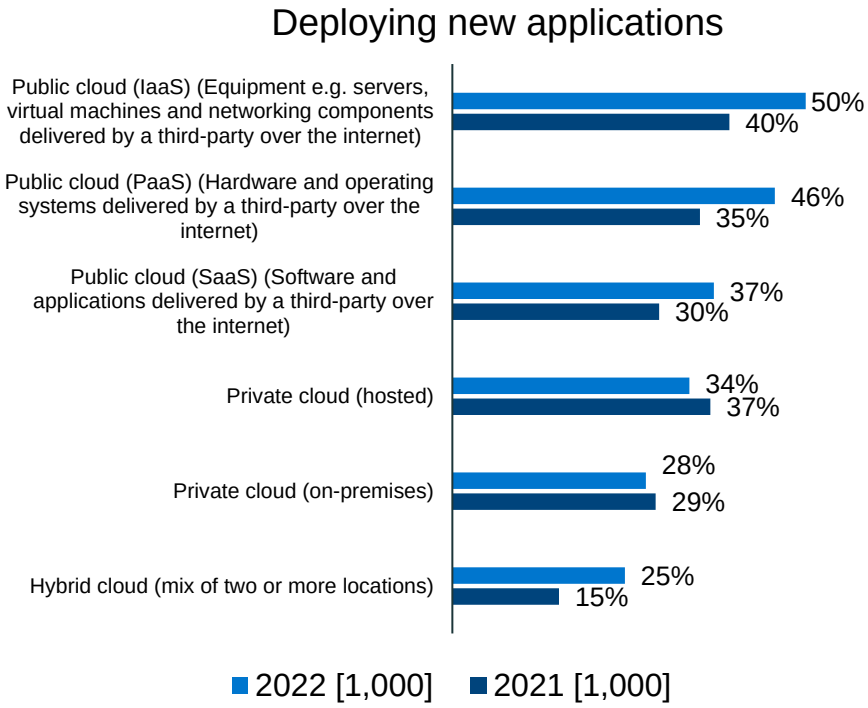
agree that **emerging technologies** (such as AI, IOT, edge) pose a **risk to data protection**



4. Securing a cloud environment

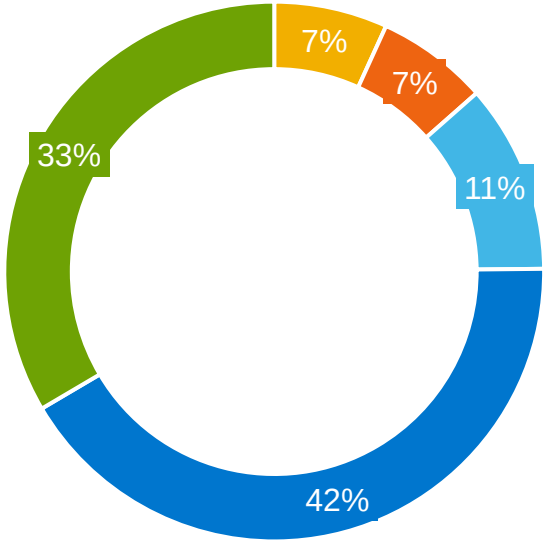
Organizations appear to be shifting towards using public cloud for updating existing and deploying new applications





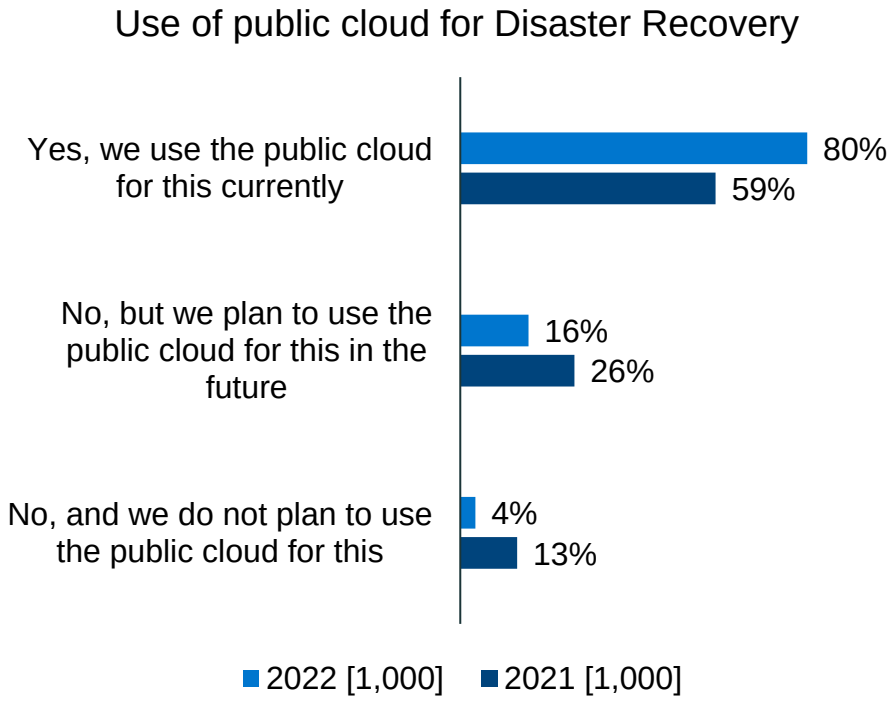
However, this shift towards public cloud may create data protection challenges for many organizations

Confidence to protect all data across public cloud environments



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

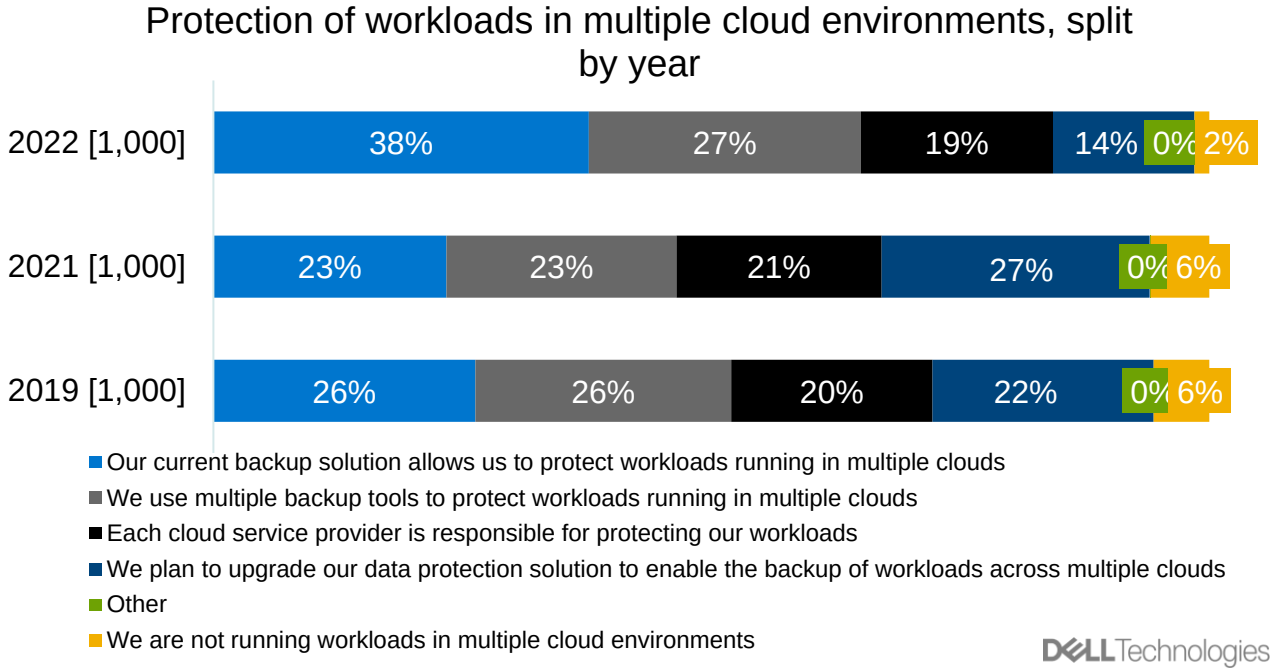
Moreover, the move from organizations planning to use public cloud for Disaster Recovery in the future is increasingly becoming a reality



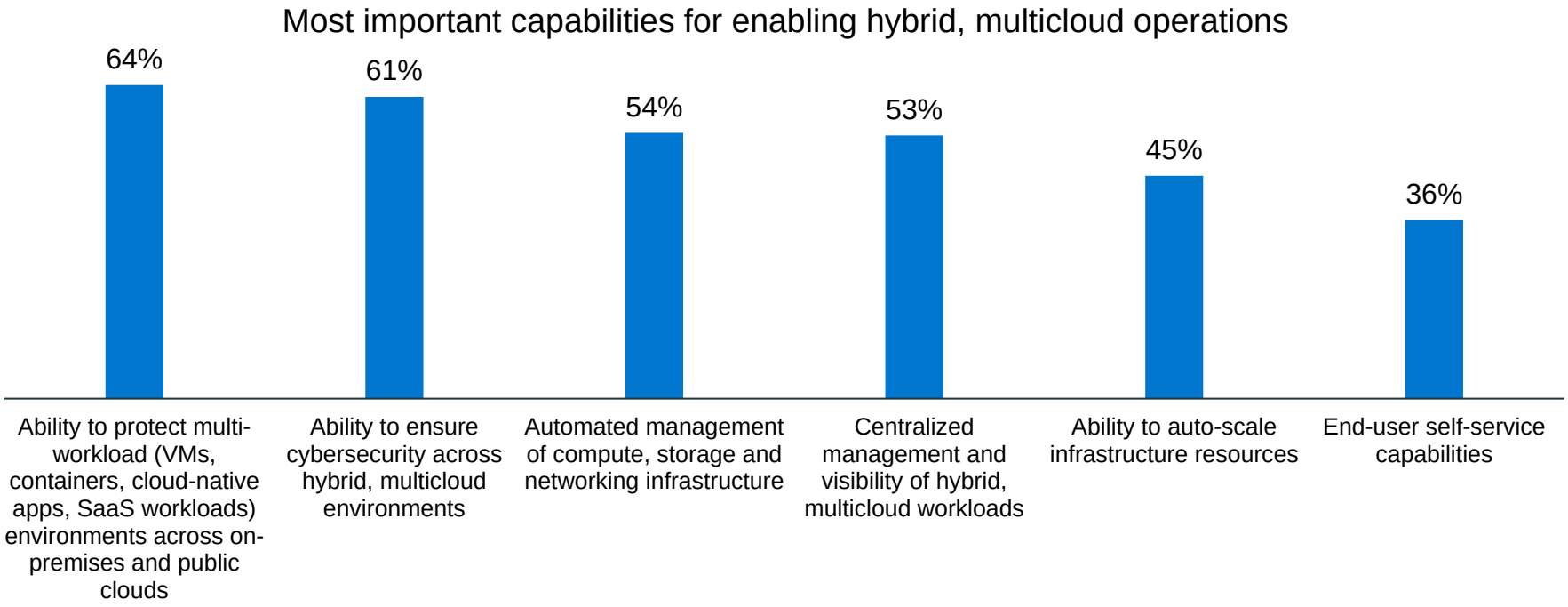
There has been a shift in how organizations plan to protect their workloads in multiple cloud environments, although a number aren't using specific solutions to protect them

19%

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



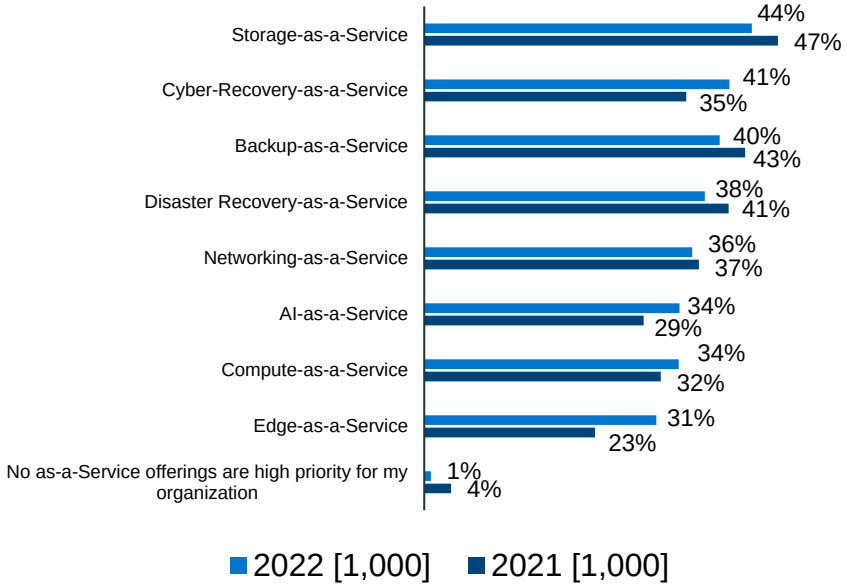
Protecting multi-workload environments and ensuring cybersecurity are most important capabilities for enabling hybrid, multicloud operations



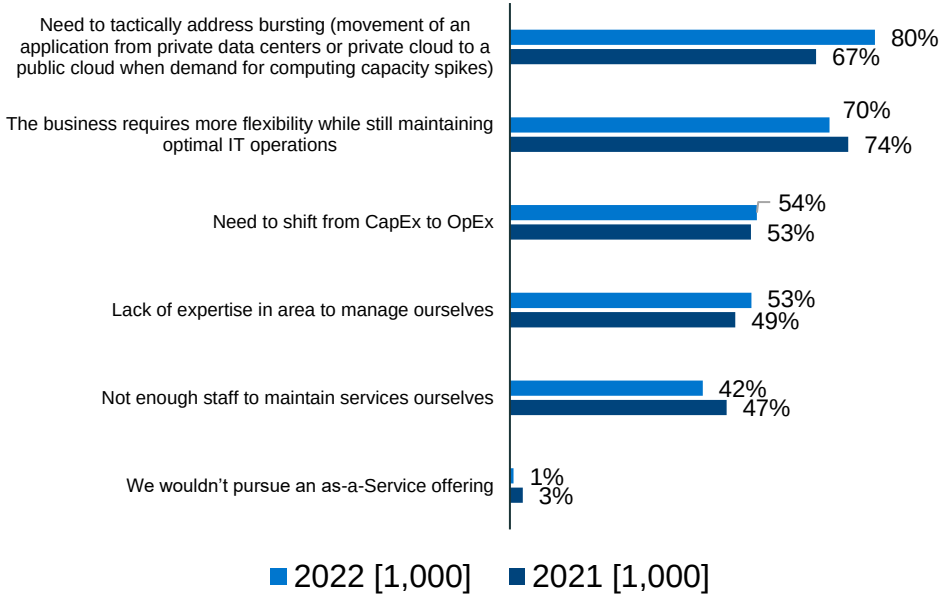
5. Looking to the future: the growth of as-a-Service

As-a-Service offerings are more likely to be a priority this year, with a greater need for tactically moving applications to public cloud

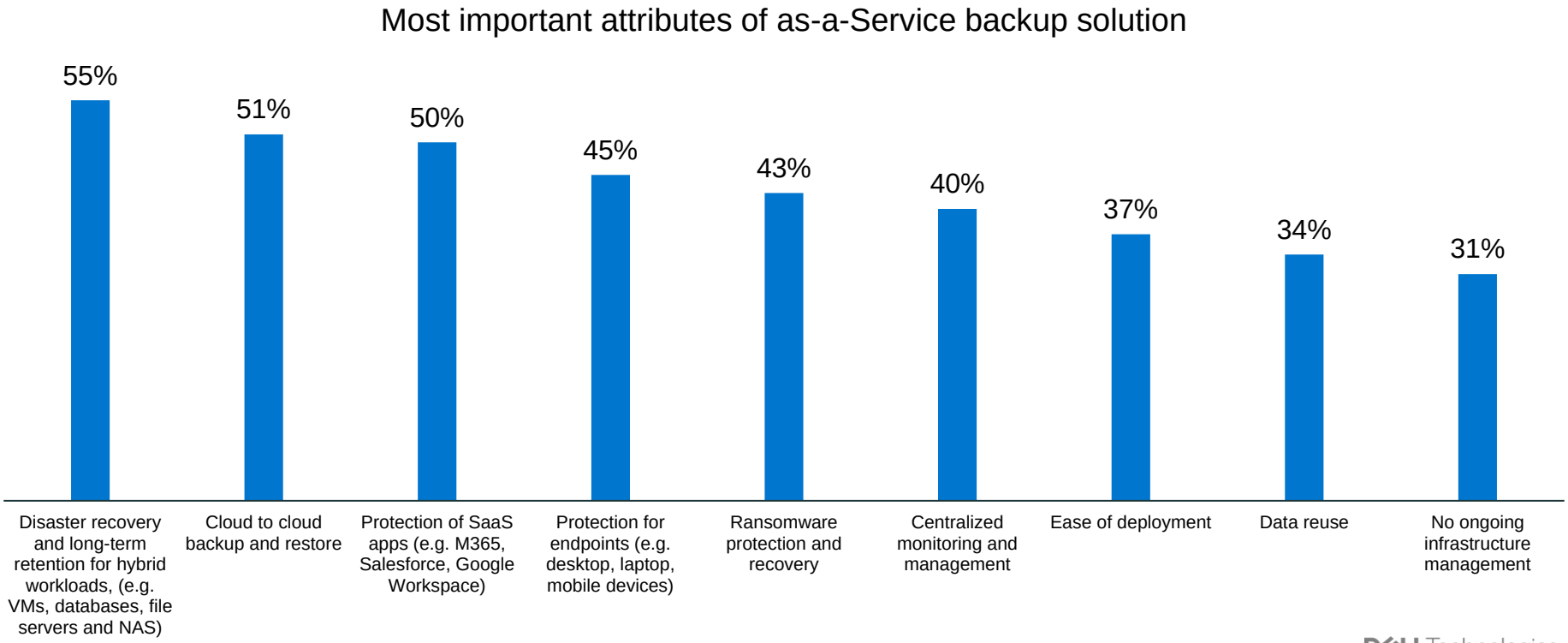
Ranked within top 3: Highest priority as-a-Service offerings, split by year



Ranked within top 3: Main reasons for pursuing as-a-Service offerings



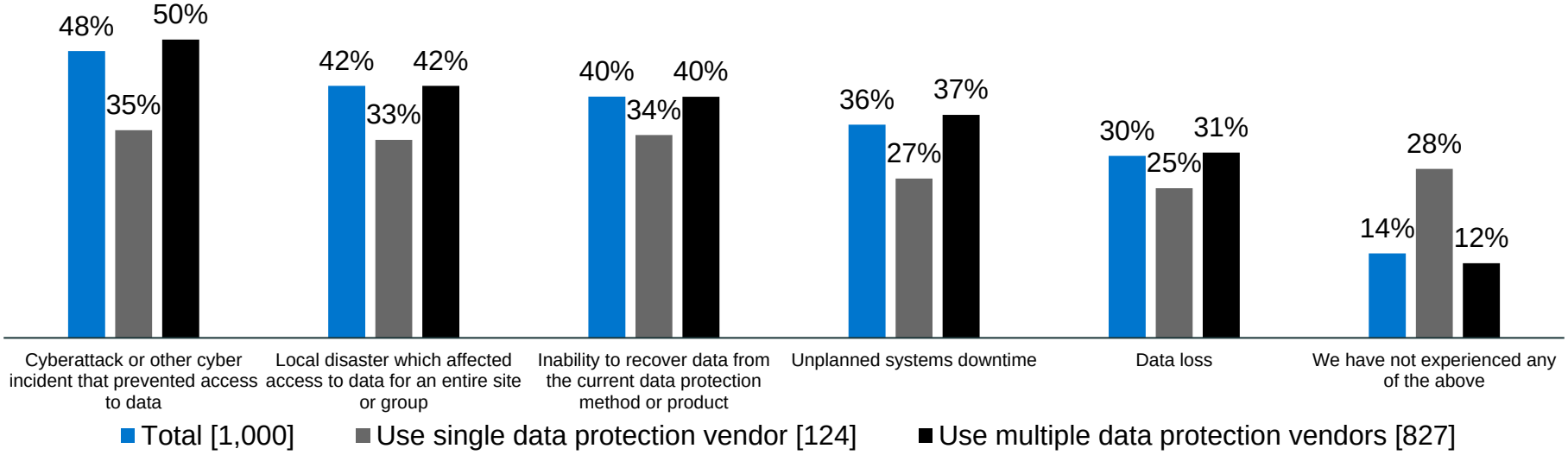
There are a range of attributes considered important for as-a-Service backup solutions



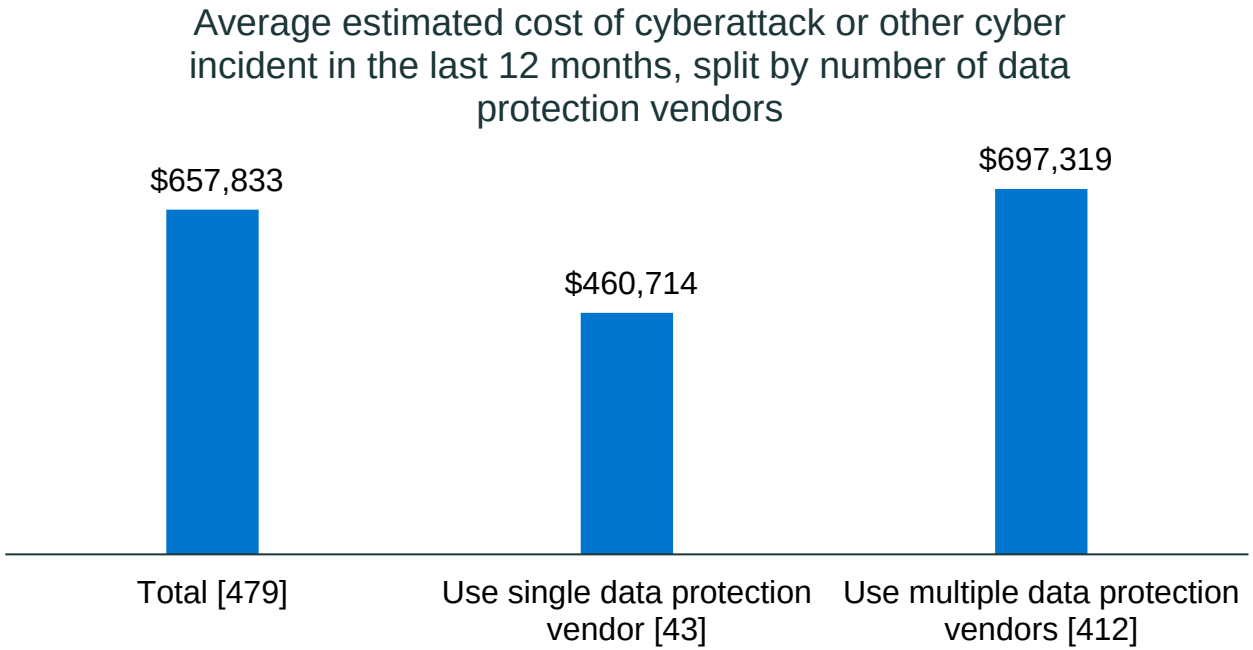
6. Simplifying data protection

Organizations using multiple data protection vendors are more likely to have suffered disruption, suggesting this approach exacerbates these challenges – particularly for cyber incidents

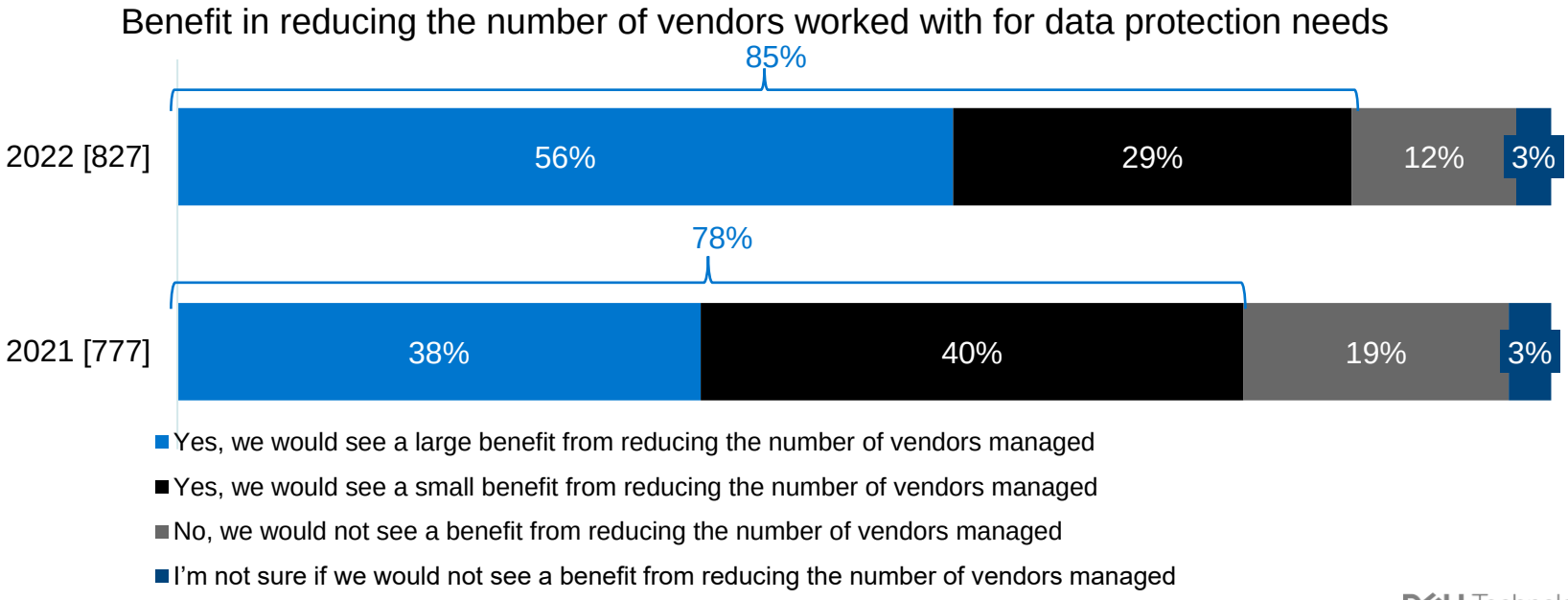
Organizations suffering various disruptions in the last 12 months, split by number of data protection vendors in use



And cyber security incidents are estimated to cost organizations who use multiple data protection vendors more than those who use a single vendor



The vast majority of those using multiple data protection vendors believe they would benefit from reducing the number of vendors they use – which has grown YoY



Key findings – in summary (1/2)

The data protection risk landscape

- Most are not very confident that they would be able to recover all systems and data to meet SLOs in the event of a data loss incident
- Many have an understanding of Zero Trust standards, yet few have fully implemented the architecture or their associated 7 tenets
- Fear that organizations will experience a disruptive event in the next 12 months is extensive, with the potential impacts financially damaging
- Such fear is likely justified with increasing levels of disruption seen YoY and encountering data protection challenges are commonplace

The increasing threat posed by cyberattacks

- Most are concerned that their organization's data protection may not be able to cope with a malware or ransomware threat, and that they have become increasingly vulnerable with more employees working from home
- Organizational confidence in recovering lost data from a cyberattack is low
- Further, many are misguided and over-confident about the likelihood and consequences of ransomware attacks
- There has been an increase in organizations suffering a cyberattack or incident in the last 12 months and security breaches have been more likely to be the cause of data loss and/or systems downtime

Protecting new and emerging tech

- Many believe that emerging 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
- The adoption of containers and cloud-native apps can help drive modernization, but most IT decision makers cite the lack of data protection solutions for these newer technologies as a challenge
- Investment in emerging technologies is a positive move for organizations, which must be accompanied by supporting and robust data protection infrastructure
- It is, therefore, encouraging to see that security in edge computing locations is on the rise

Key findings – in summary (2/2)

Securing a cloud environment

- Organizations have moved towards the use of public cloud for updating existing and deploying new applications, and disaster recovery
- However, few are very confident that their data will be protected across their organization's public cloud environment, and this could create data protection challenges for many
- Organizations need to ensure they have specific solutions in place to protect data across multicloud workloads, as some still believe their cloud providers are responsible for this
- Considering the landscape, it is encouraging that organizations consider protecting multi-workload environments and ensuring cybersecurity as the most important capabilities for enabling hybrid, multicloud operations

Looking to the future: the growth of as-a-Service

- As-a-Service solutions are more likely to be a priority this year, and probable in forming part of many organizations' data protection solutions in the future
- Storage, cyber-recovery and backup are organizations' top three priorities for as-a-Service offerings

Simplifying data protection

- Organizations using a single data protection vendor are less likely to have suffered disruption in the past year compared to those using multiple vendors, particularly those related to cyberattacks or other cyber incidents
- These cyber incidents are also estimated to be more costly to those using multiple protection vendors, on average
- Most organizations using multiple data protection vendors believe they would see benefit in reducing the number of vendors – and this sentiment has increased this year

Mitigate risk and get ahead of the curve

Dell Technologies point of view

Modernize your data protection

Reduce operational complexity

Enhance cyber resiliency

Learn more at dell.com/GDPI


DELL Technologies