Global Data Protection Index - Special Edition 2024

Key Findings - October 2023

VansonBourne

DELL Technologies

Focus of key findings

1
The data protection risk landscape

2
The increasing threat of cyberattacks

3
The use of multicloud

4
Securing a cloud environment

Five key takeaways

Cyber-attacks continue to be on the rise

The cost of cyber-attacks is increasing

Insurance policies are not covering enough of the cost of attacks

Increased use of GenAI could lead to more high value data

Leading to greater risks and more financial impacts of cyber-attacks

Who did we interview?

1,500 IT and IT security decision makers were interviewed in September and October 2023

Organizations from a wide range of public and private industries

Organizations with 250+ employees

4 regions:

Americas (300)
EMEA (675)
APJ (375)
China (150)

1. The data protection risk landscape

Concerns over data protection measures are widespread, and with confidence lacking, organizations find themselves in a vulnerable position

60%

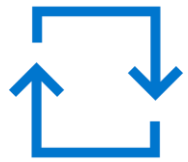
are **not very confident** that their organization is **meeting its backup and recovery service level objectives (SLOs)**

79%

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

75%

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



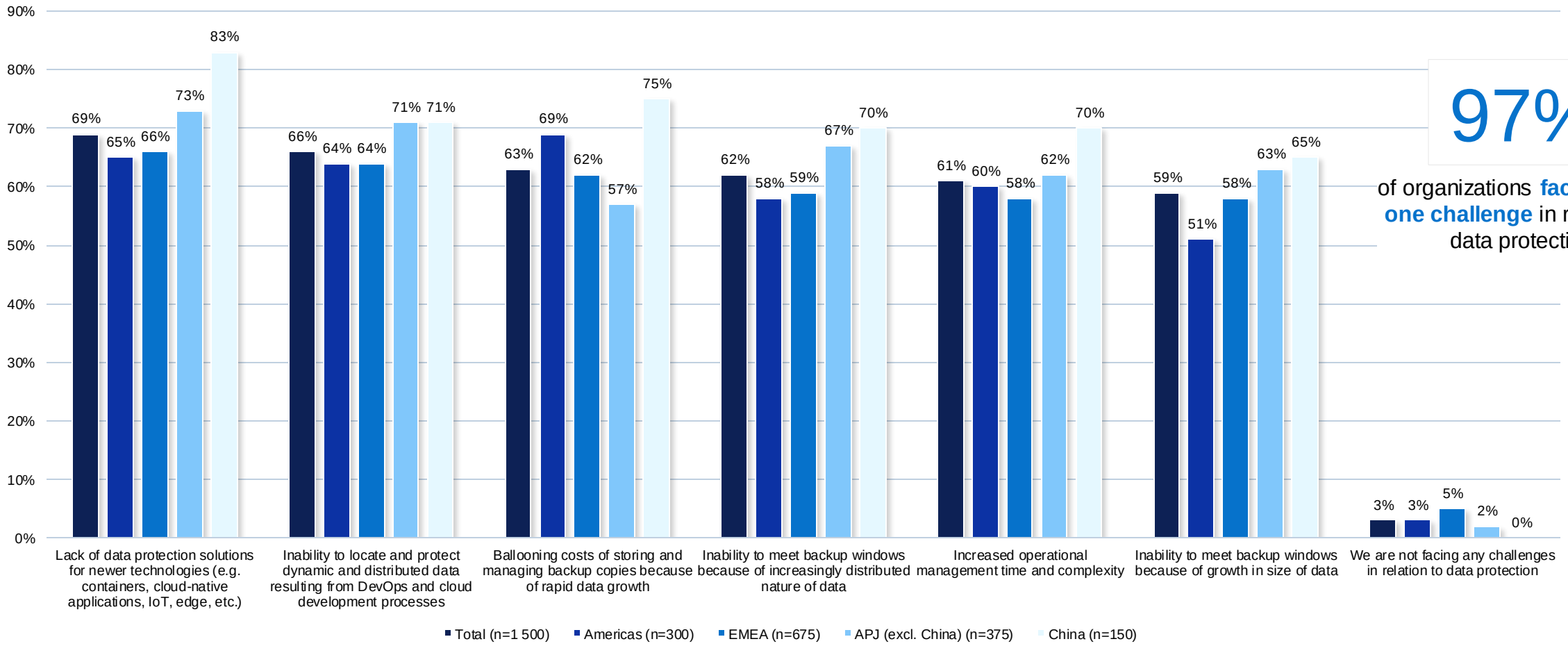
65%

are **not very confident** that their organization could fully **recover systems/data from all platforms** in the event of a data loss incident

DELL Technologies

In addition to concerns over data protection, many organizations face challenges

Ranked top 5: Challenges faced in relation to data protection, split by region

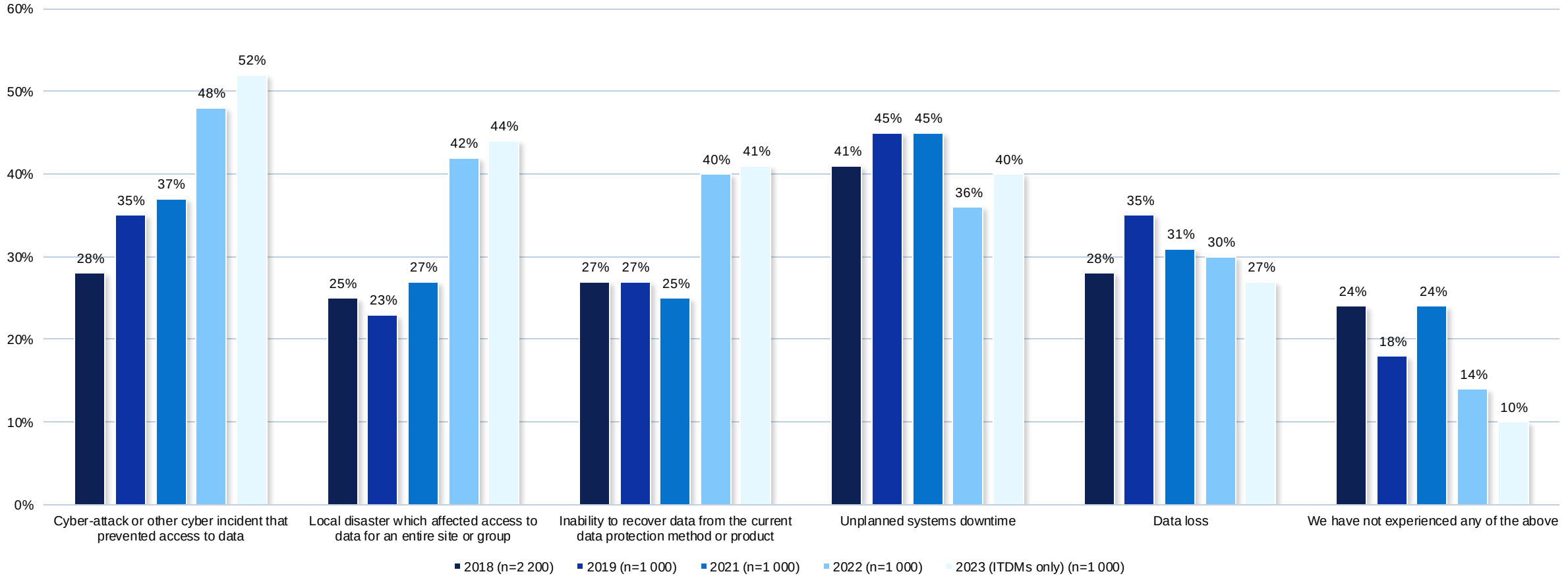


97%

of organizations **face at least one challenge** in relation to data protection

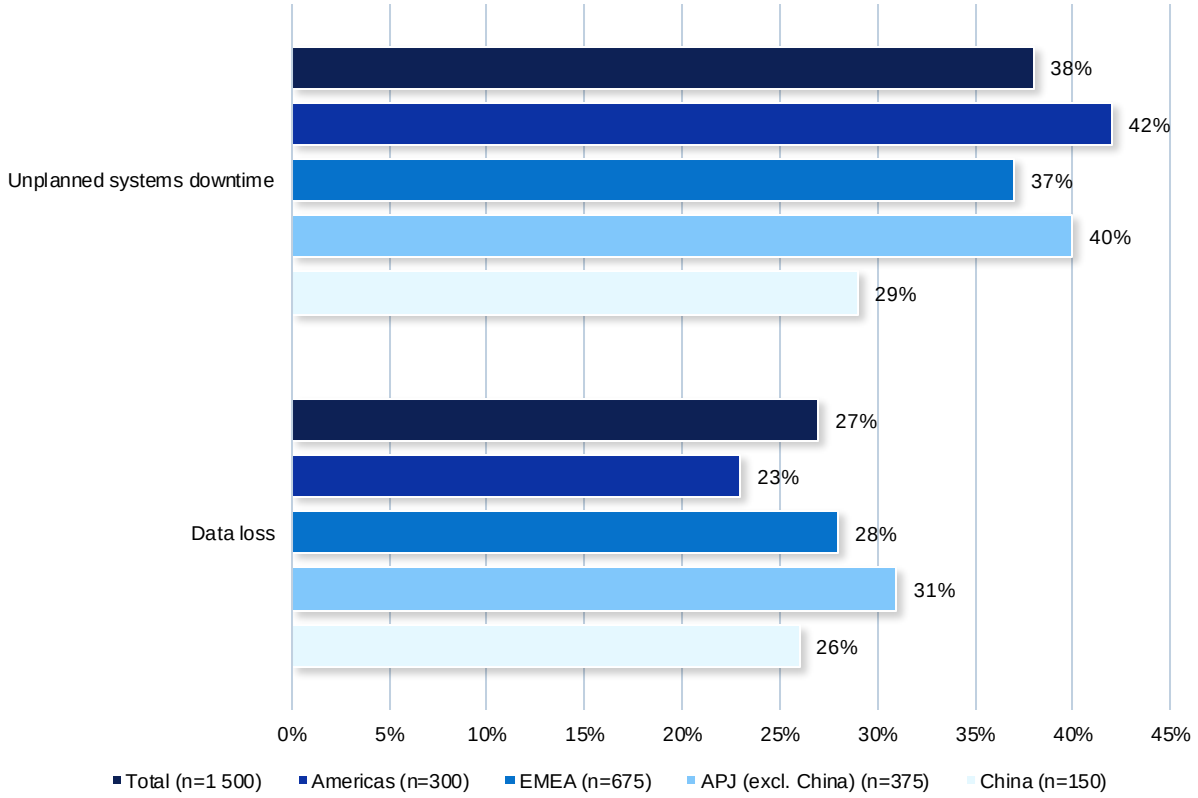
In the last 12 months organizations have faced significant disruption, with cyber-attacks posing an ever present and increasing threat

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



Data loss has not only contributed to disruption, but has also impacted the bottom line

Percentage of organizations that have experienced unplanned systems downtime or data loss in the last 12 months, split by region



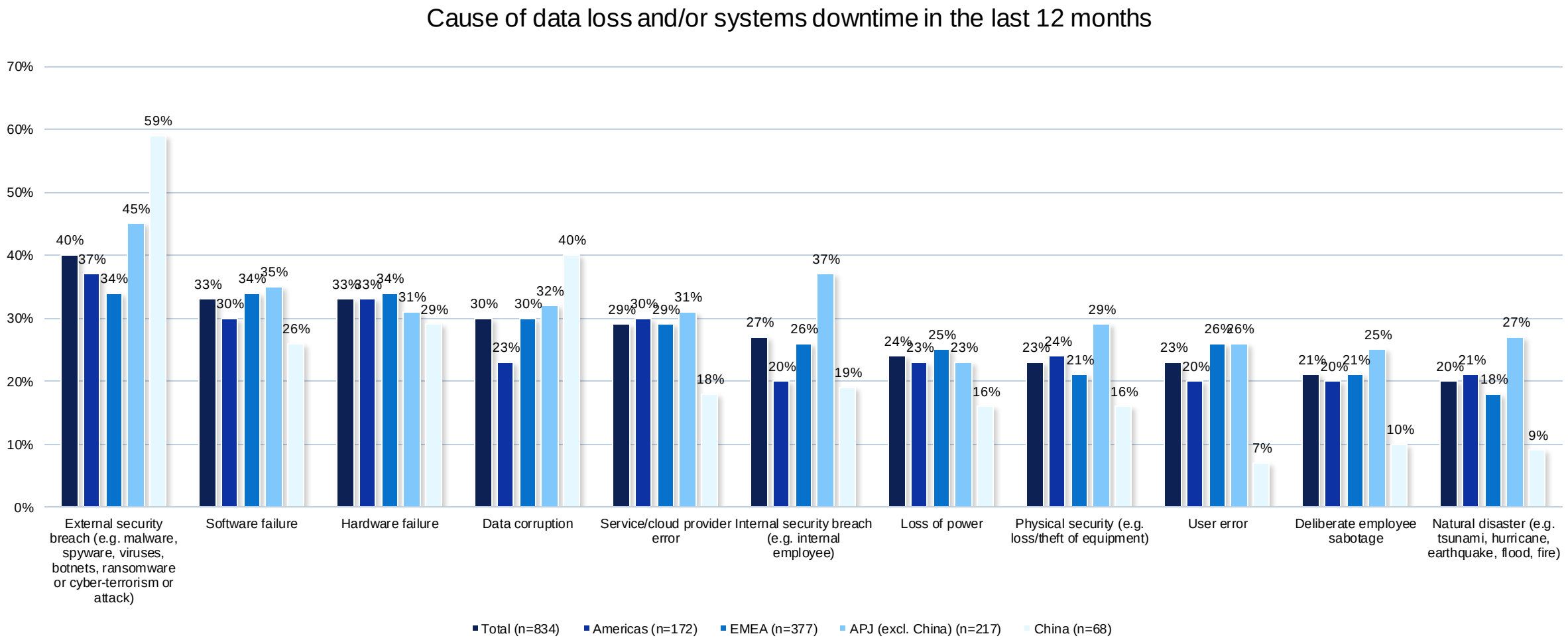
In the last 12 months:

26 hours **of unplanned systems downtime**, experienced on average

2.45TB **worth of data** has been lost, on average

$2.61 million, the average **cost of data loss**

External security threats are the most common causes of data loss and/or unplanned systems downtime over the last 12 months

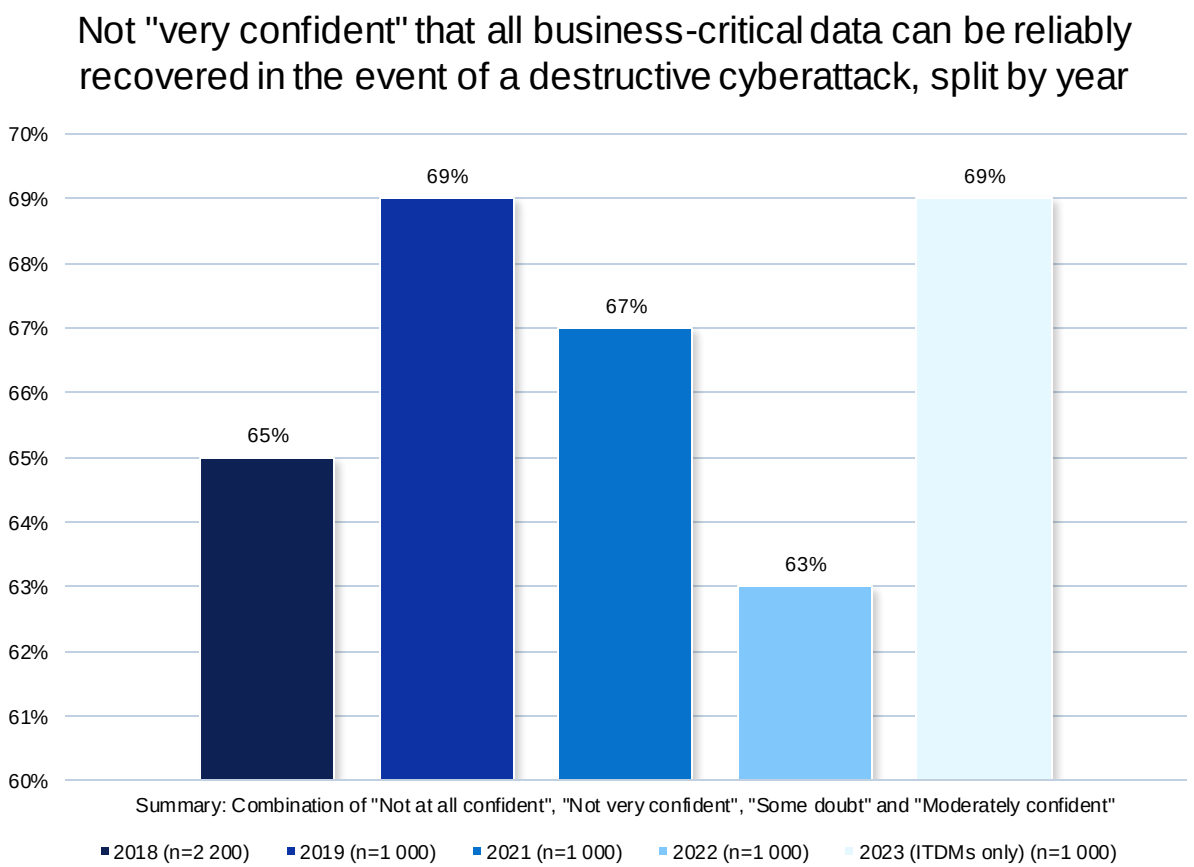


Despite the challenges and concerns over data protection, few have fully implemented Zero Trust security

Filter: Data Split: Region = Total

2. The increasing threat of cyberattacks

Concerns over data protection measures are widespread, and with confidence lacking, organizations find themselves in a vulnerable position



81%

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

74%

are **concerned** their backup data could become **infected or corrupted by ransomware attacks**

Adding to the risk, there is a misguided over-confidence surrounding the consequences of a ransomware attack

72%

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

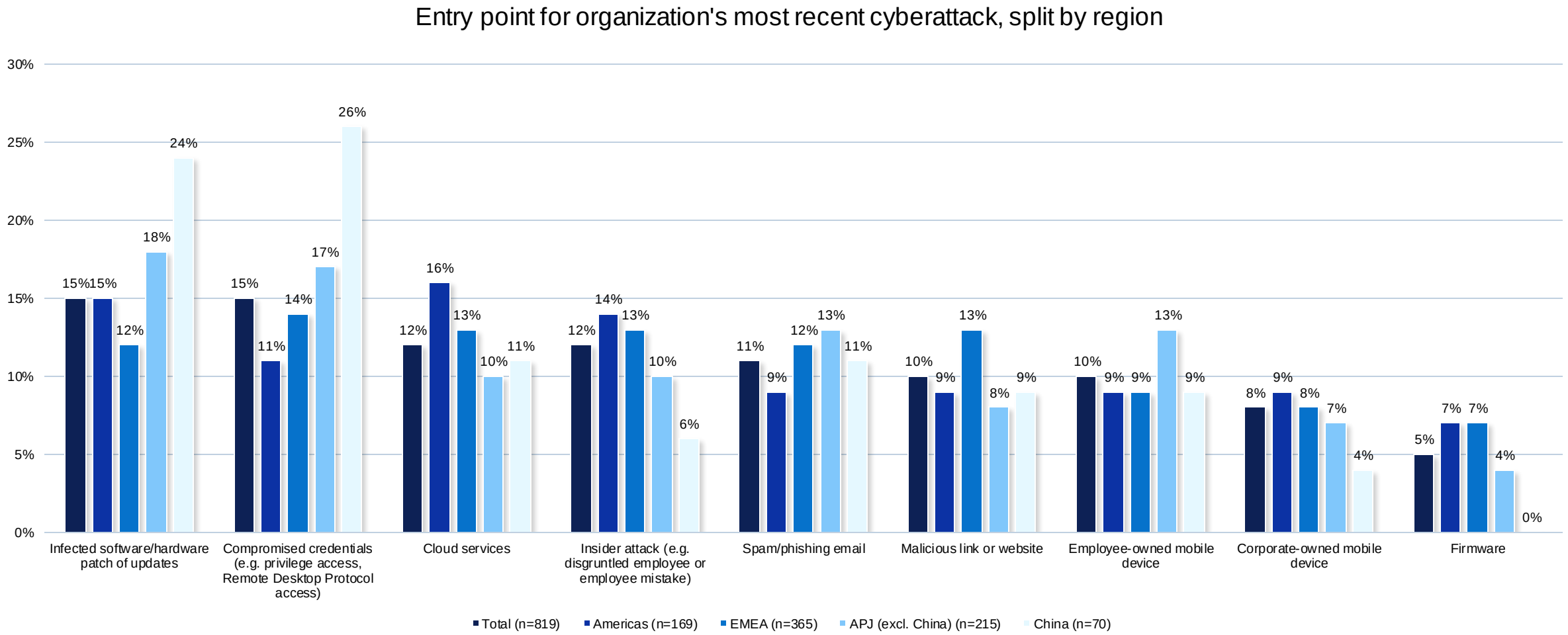
74%

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

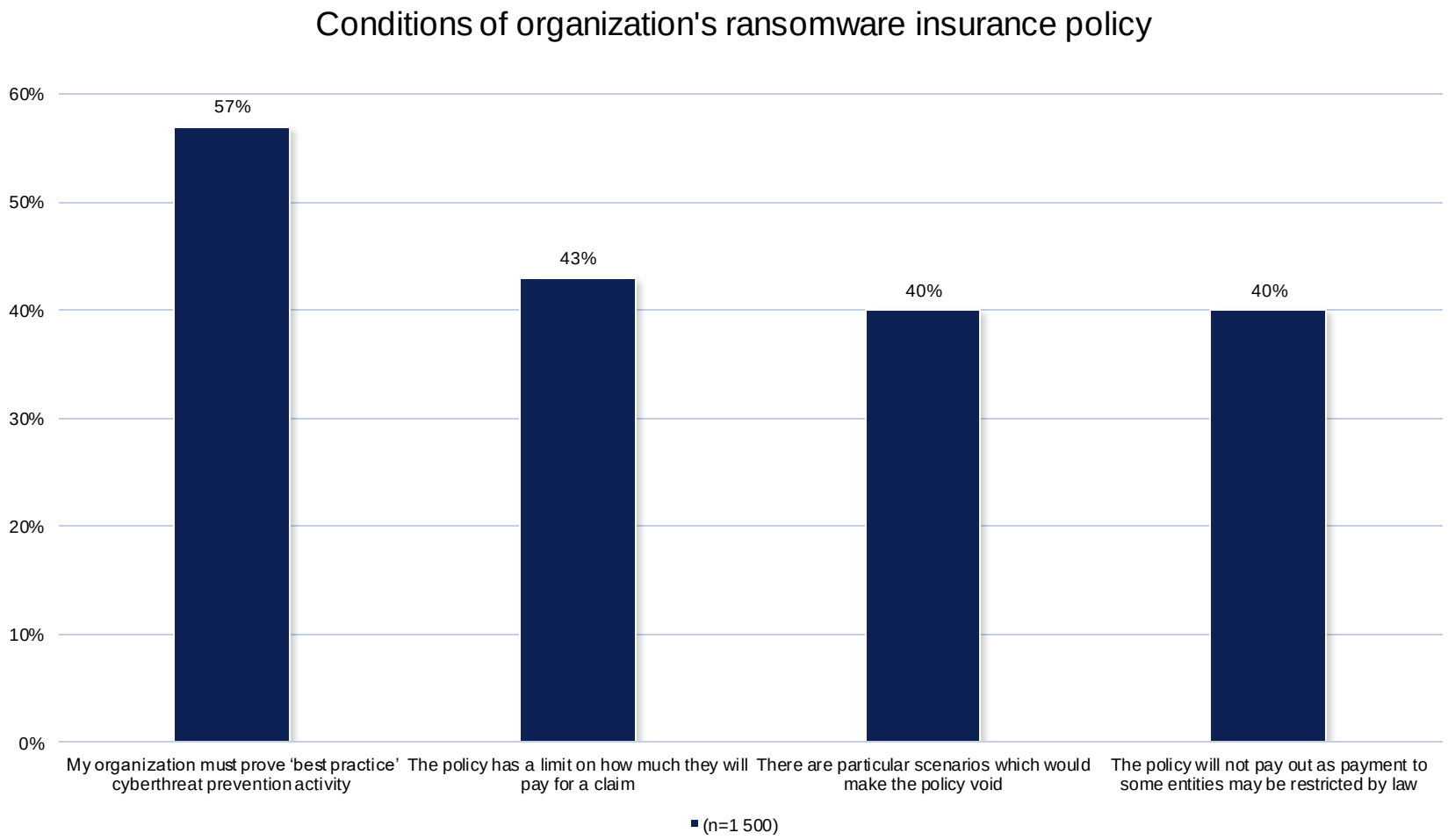
66%

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

Cyber criminals target various entry points, with attacks more likely to come from external sources



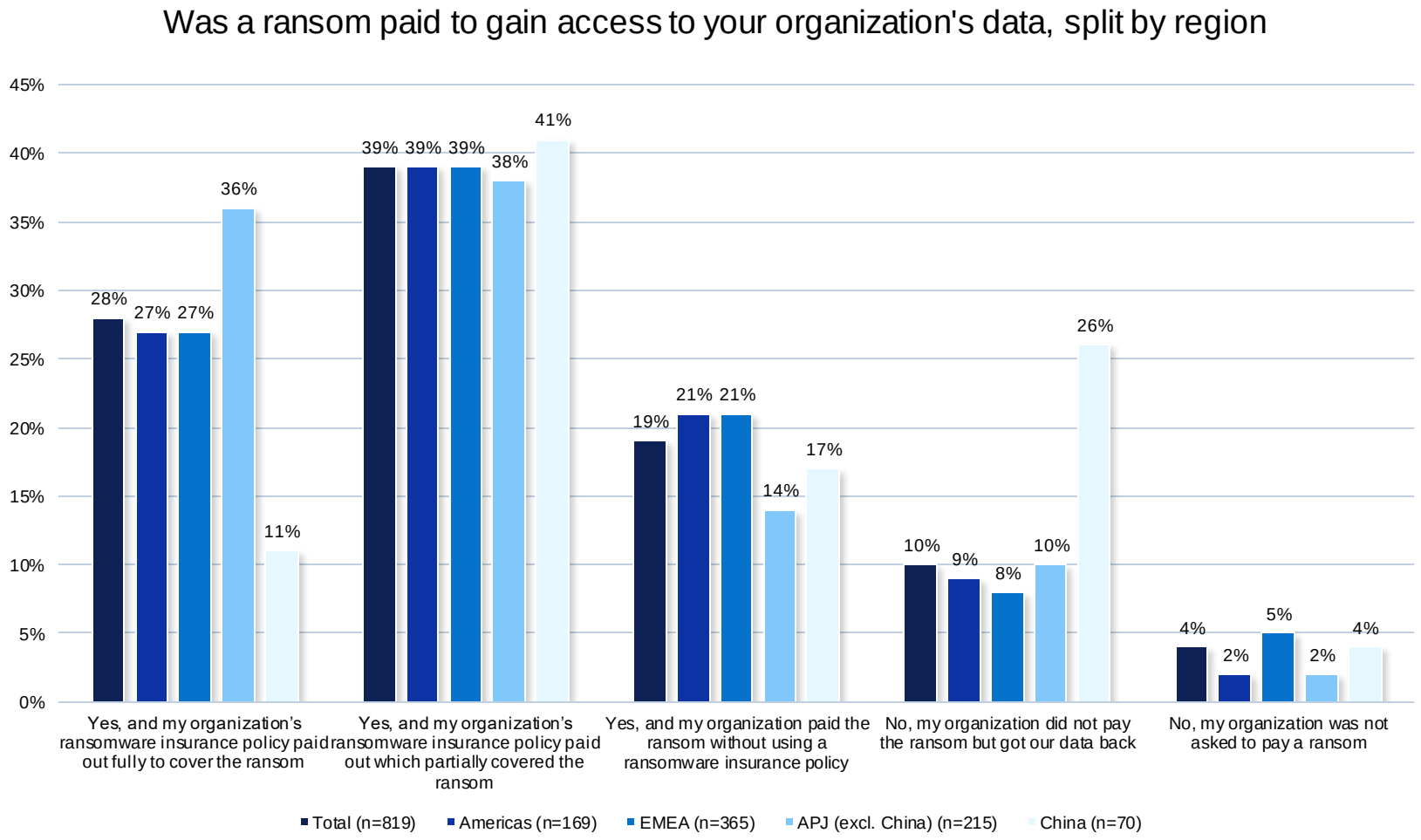
Ransomware insurance policies are commonplace among organizations, but come heavily caveated



93%

of organizations **have a ransomware policy**

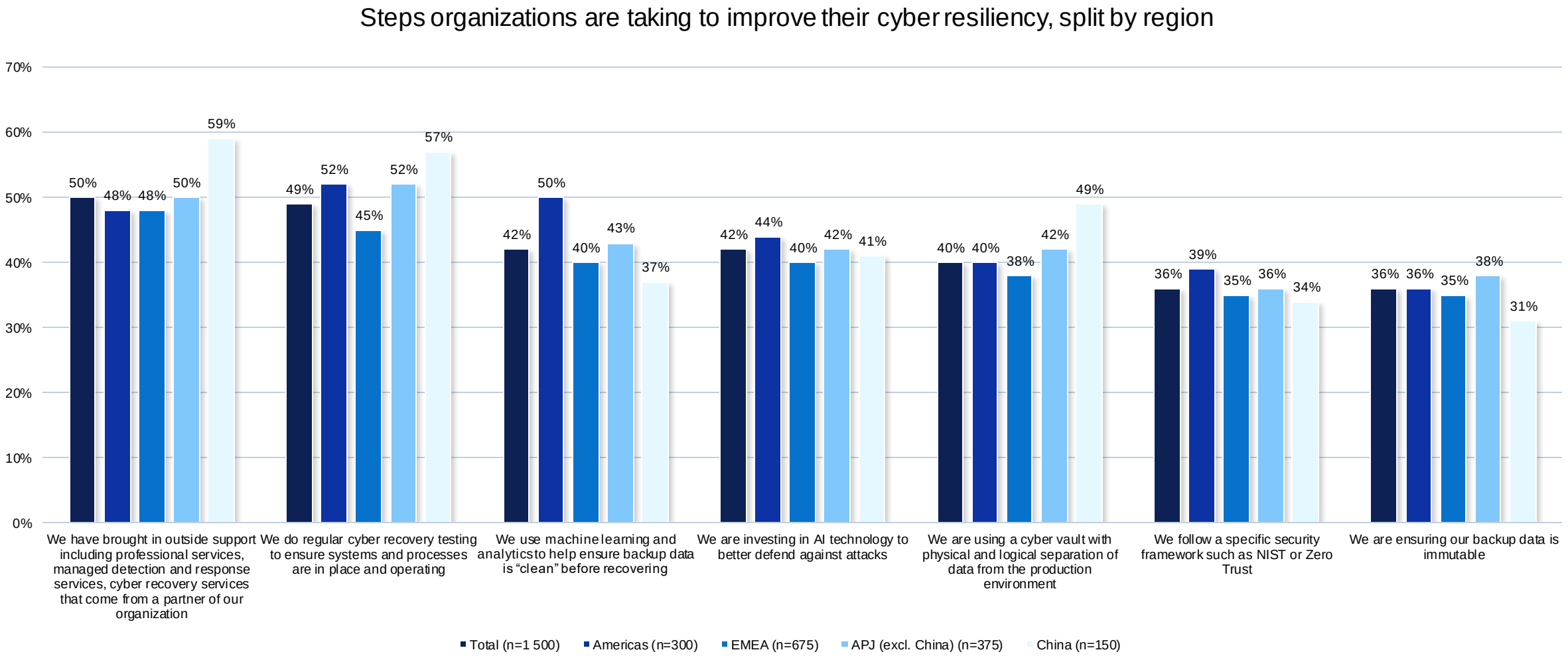
Despite many having ransomware policies in place, organizations still find themselves financially vulnerable



$1.92

million - the average cost to organizations in the past 12 months, caused by **cyber-attacks and other cyber-related** incidents

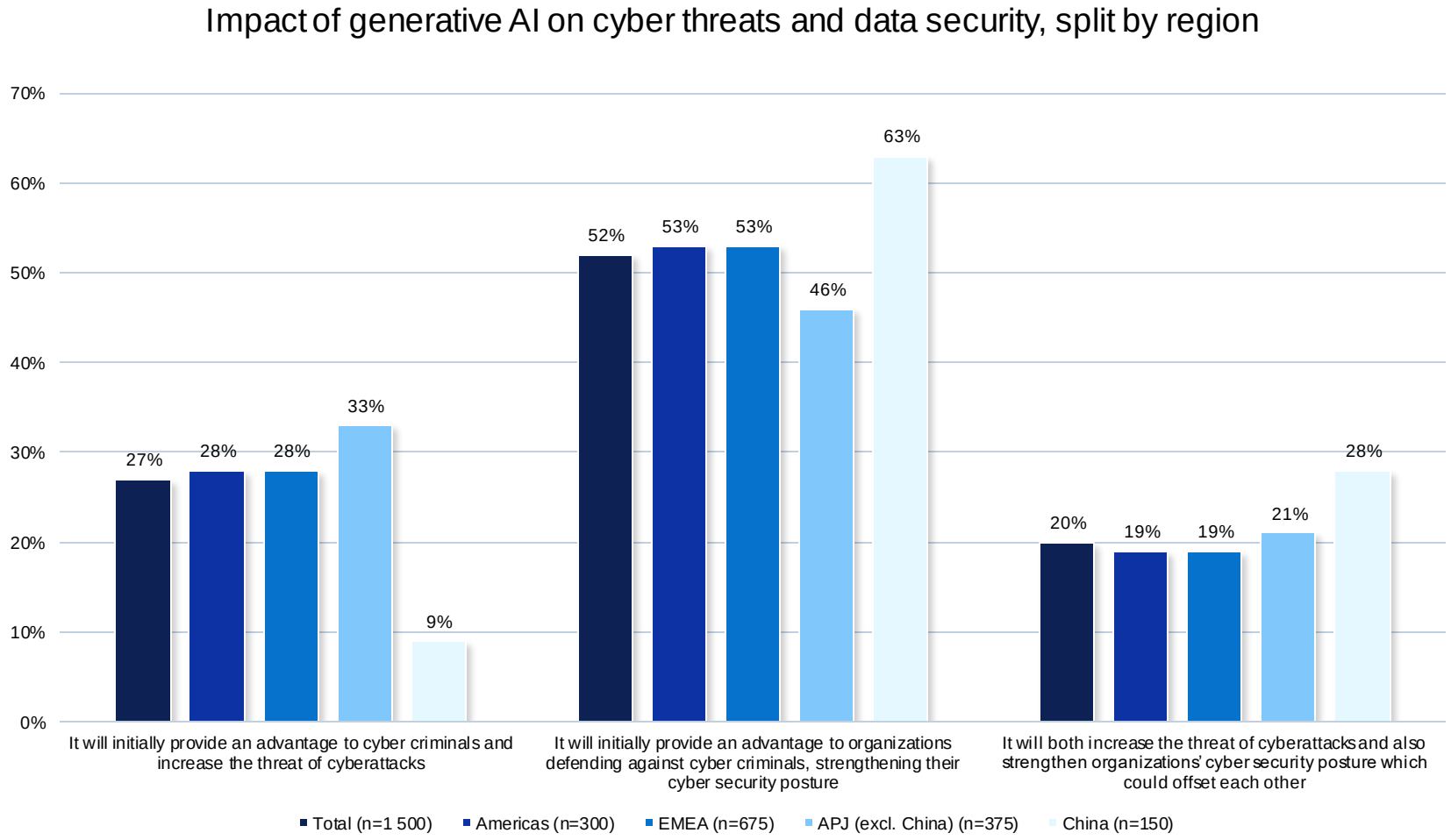
Encouragingly, organizations are taking steps to becoming more cyber resilient



However, not all believe generative AI will benefit their cyber resiliency

81%

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



In fact, with organizations already concerned over data protection, many believe generative AI will create new challenges

88%

agree that generative AI will create large volumes of new data that will **need to be protected and secured**

88%

agree that generative AI will increase the value of certain data types which would **require higher data protection service levels**

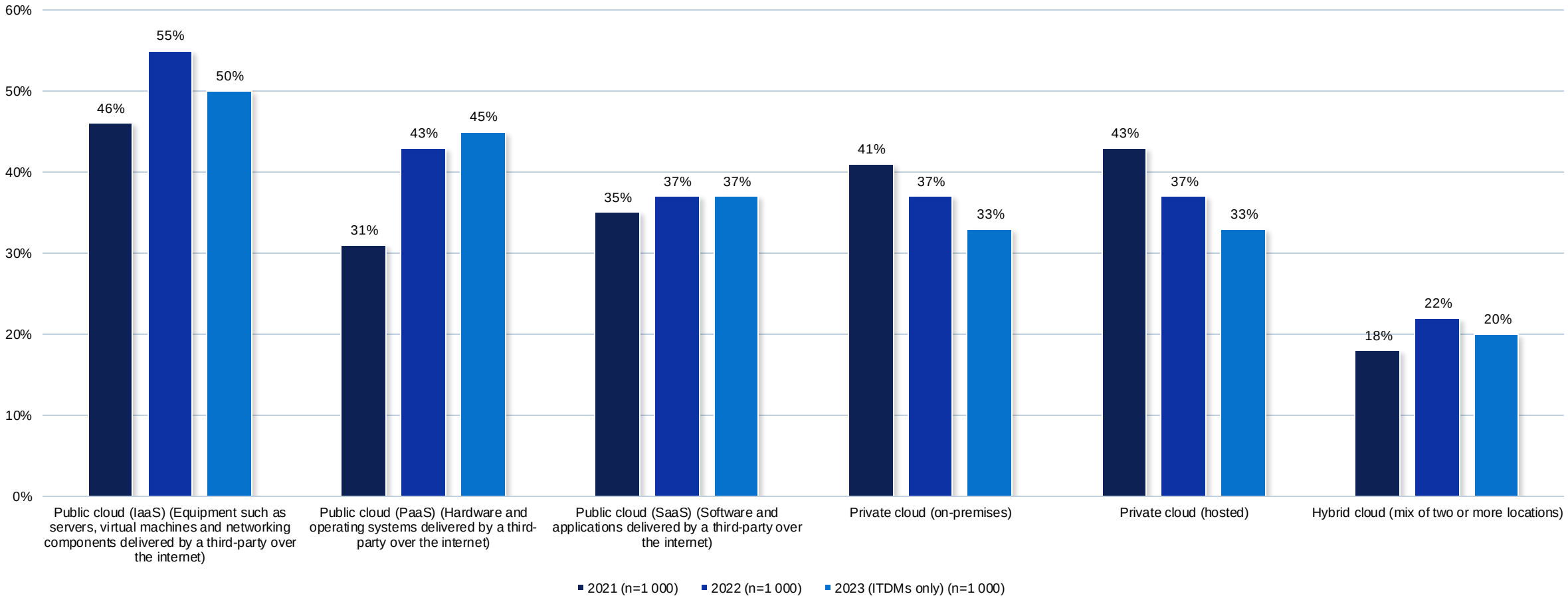
85%

agree that if data sets used for generative AI are **corrupted** it will **impact the generative AI output**

3. The use of multicloud

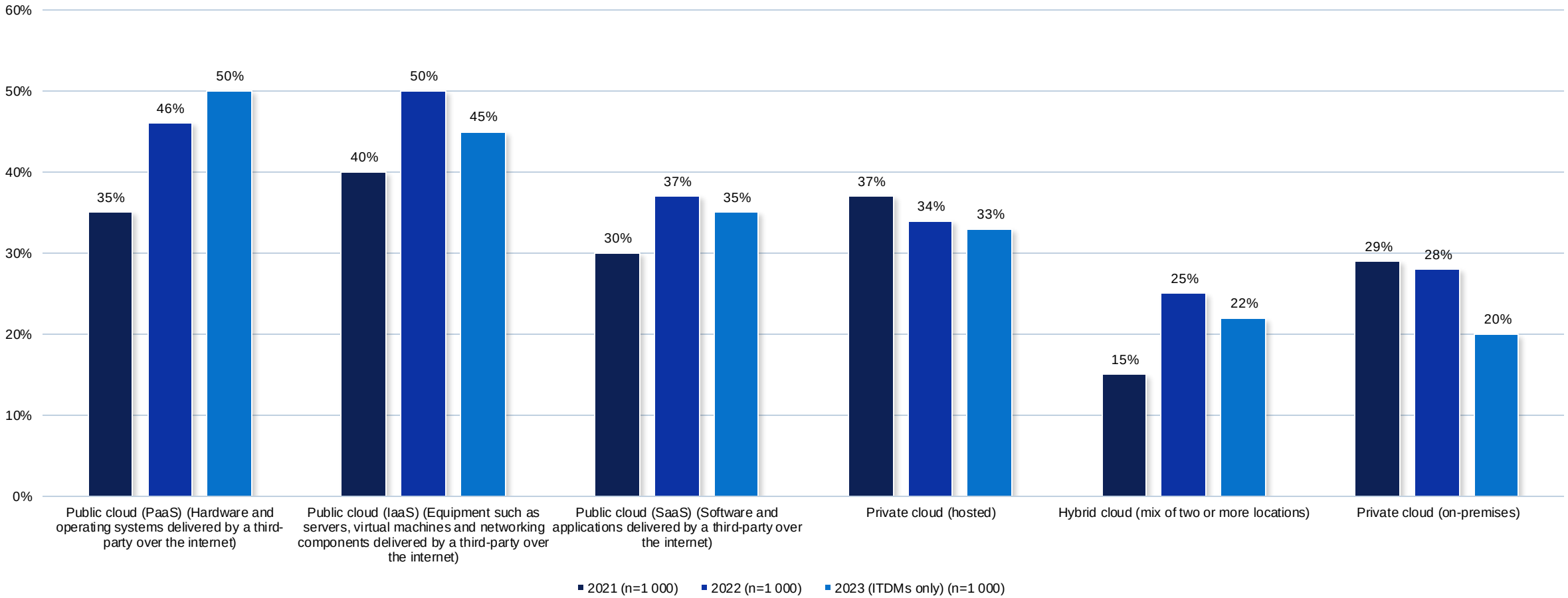
Public cloud remains a popular choice when updating existing applications, while the preference for private cloud is decreasing

Directions being taken when updating existing applications, split by year

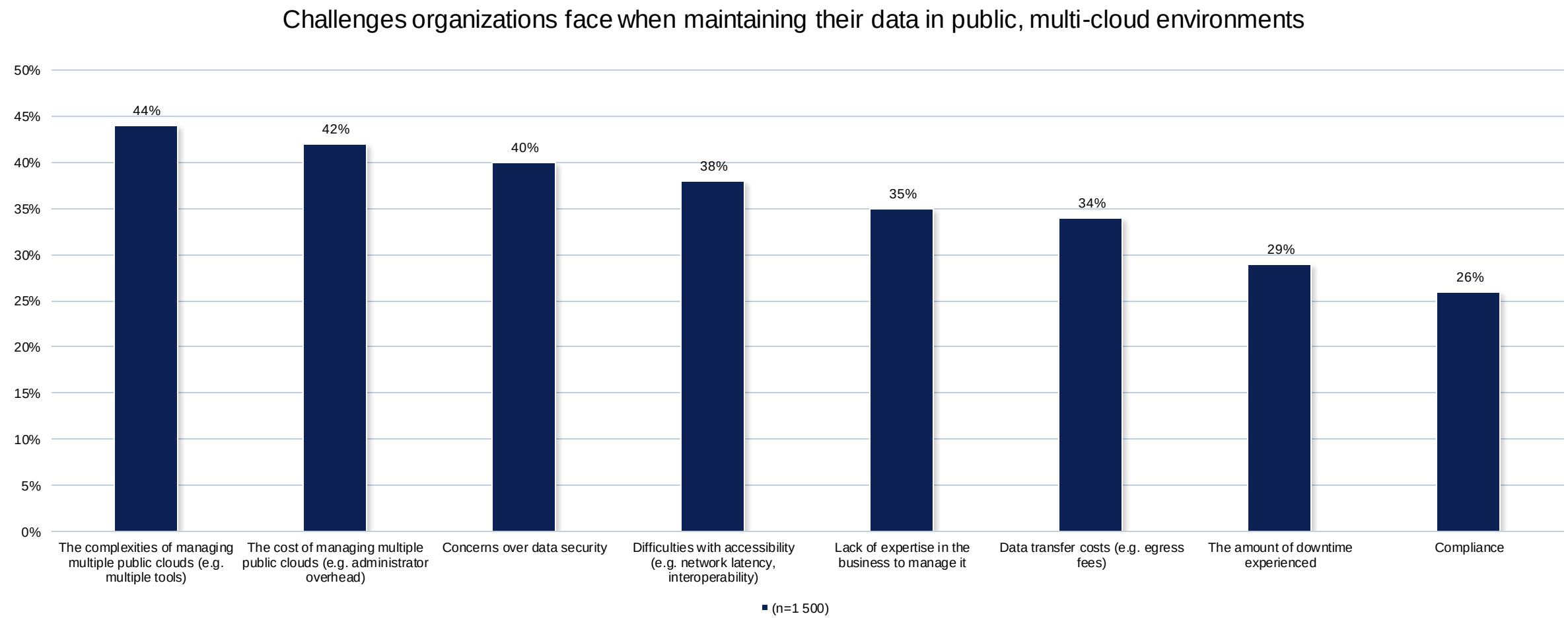


Public cloud also remains a popular choice for deploying new applications, but support may be in decline

Directions being taken when deploying new applications, split by year

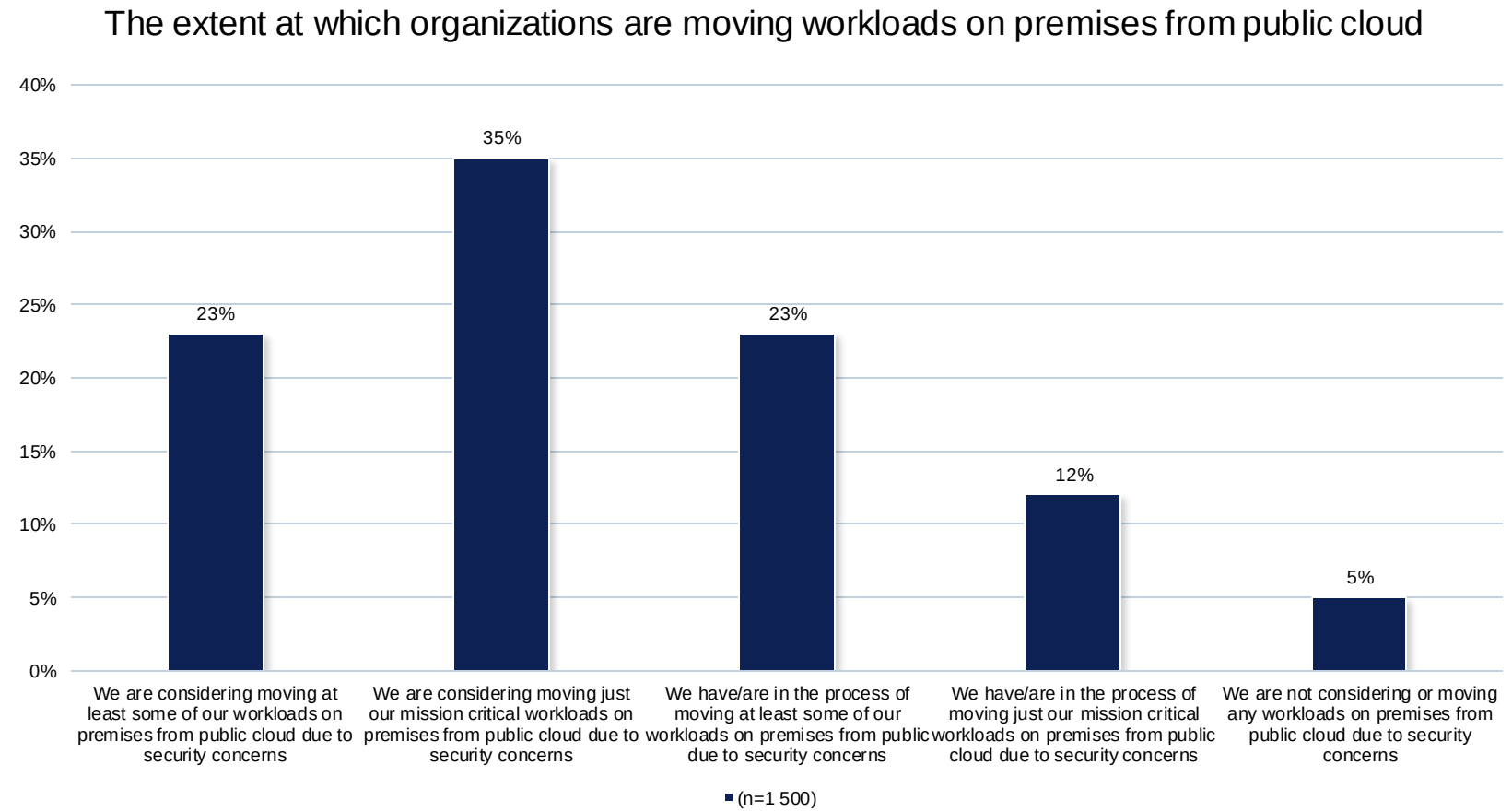


Despite the popularity of public cloud, many organizations face challenges when maintaining their data



Filter: Data Split: Region = Total

Due to security concerns many organizations are moving, or are considering moving, a portion of their workloads on premises from public clouds



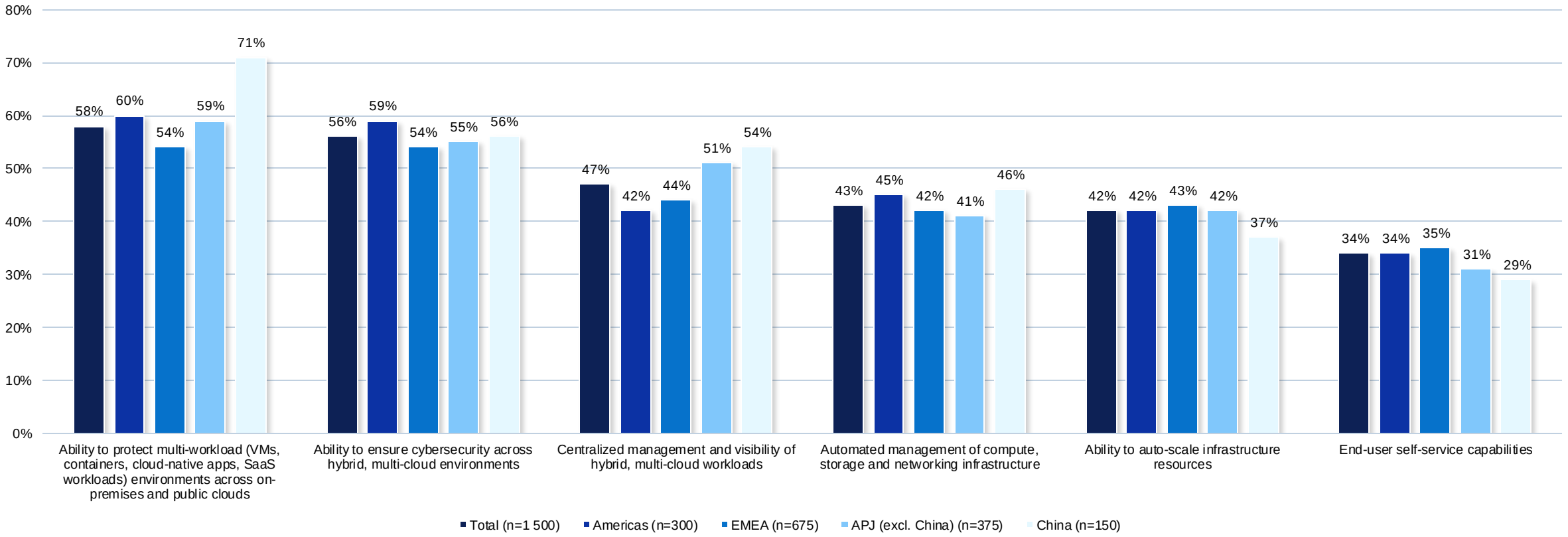
Filter: Data Split: Region = Total

79%

are **not very confident** that their organization can **protect all of its data** across public cloud environments

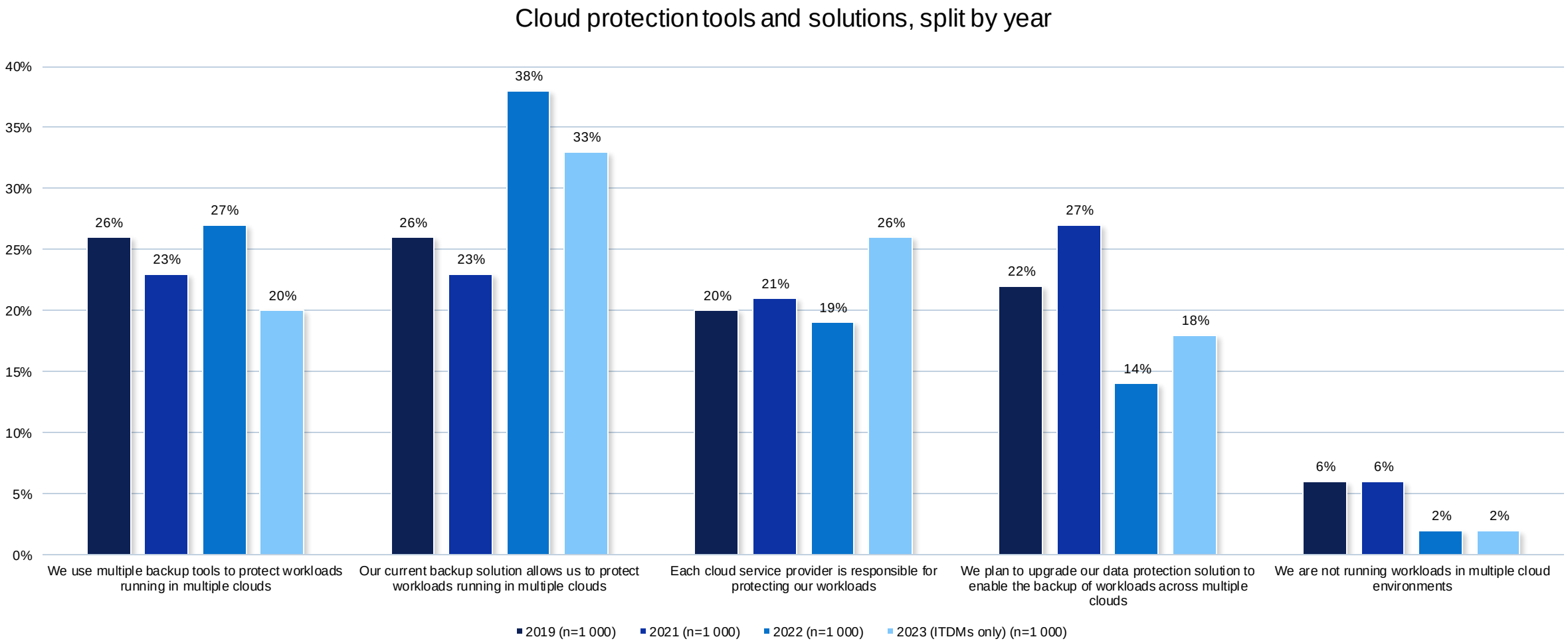
With cyber-related incidents on the rise, and confidence in data protection strategies low, many see security as the most important capability when enabling hybrid, multi-cloud operations

Most important capabilities when enabling hybrid, multi-cloud operations, split by region



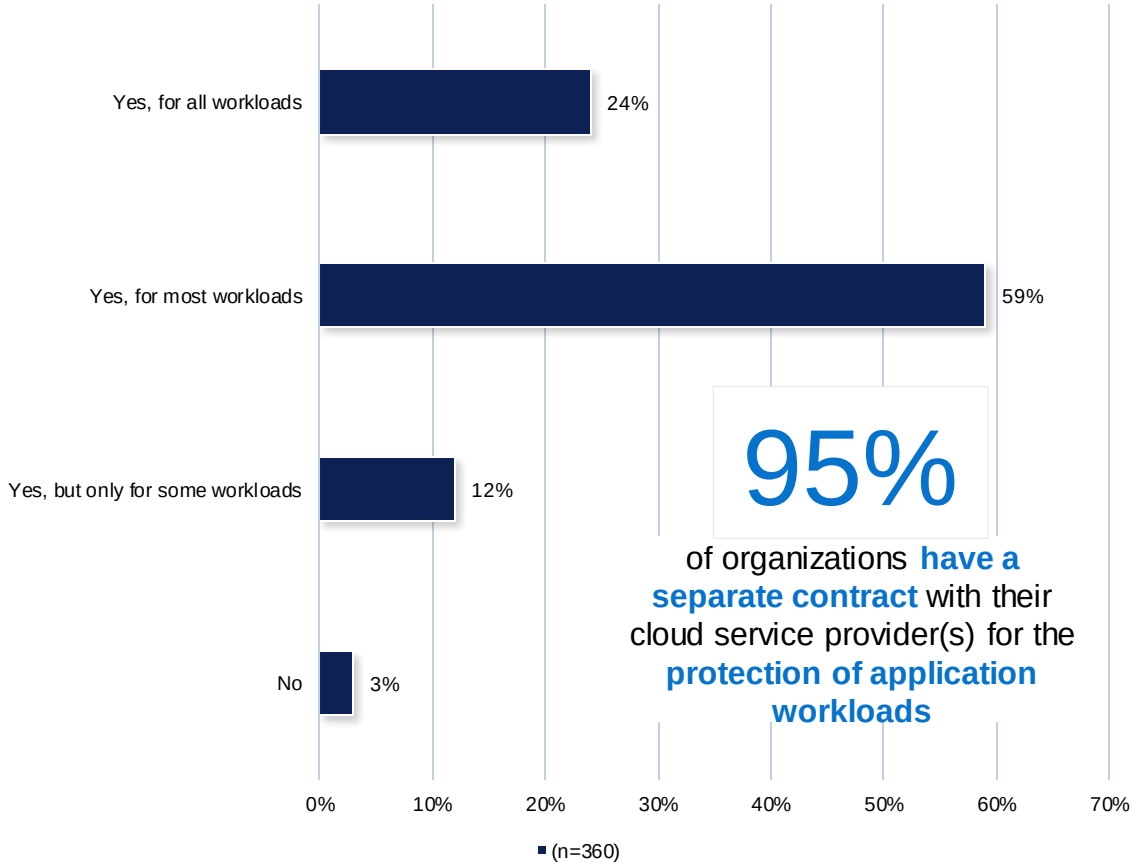
4. Securing a cloud environment

Organizations currently use various backup tools and solutions to protect their workloads, but the need for upgrades are noted



Organizations are becoming increasingly reliant on cloud service providers to protect their workloads across cloud environments

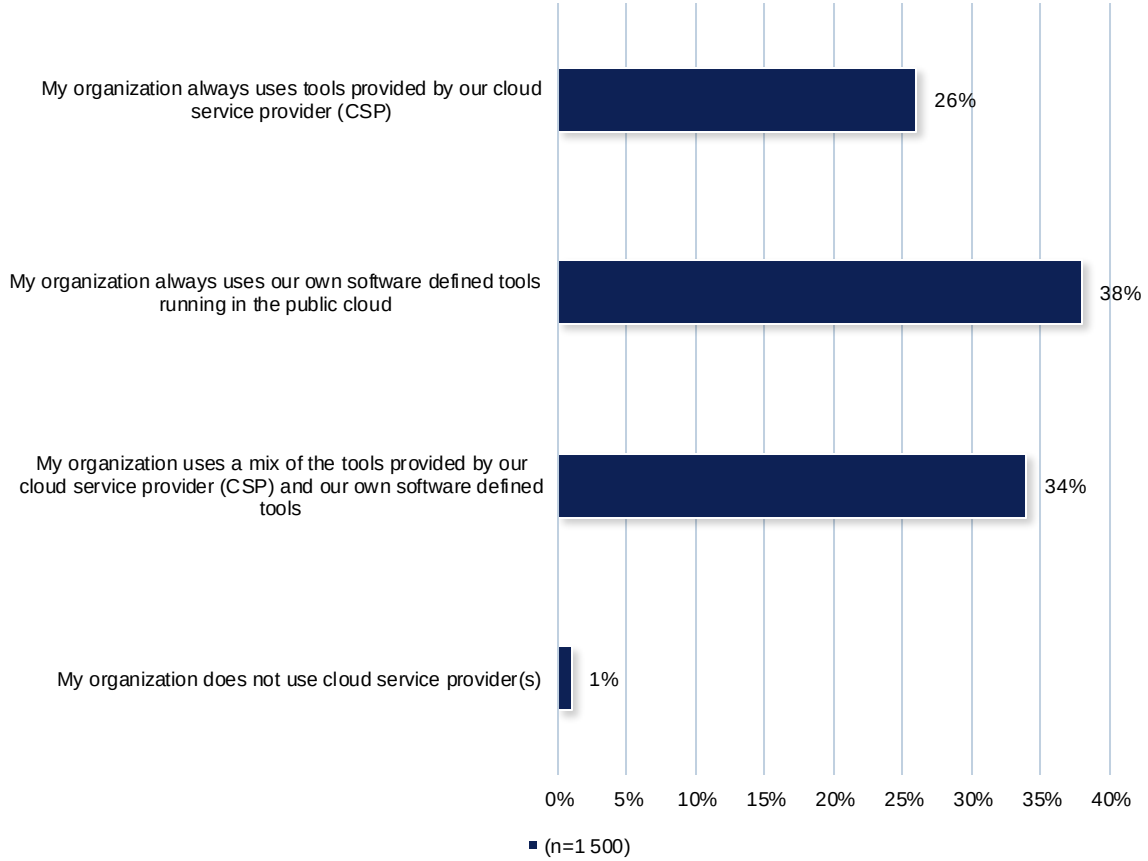
Separate contract with CSP for the protection of application workloads



95% of organizations **have a separate contract** with their cloud service provider(s) for the **protection of application workloads**

Filter: Data Split: Region = Total

Backup and recovery tools supplied by cloud service provider



Filter: Data Split: Region = Total

Key findings - in summary

The data protection risk landscape

- Concerns over data protection measures are widespread, and with confident lacking, organizations find themselves in a vulnerable position
- Nearly all organizations face challenges in relation to their data protection, with many also experiencing significant disruption over the last 12 months organizations due to data loss and/or unplanned system downtime
- External security threats have been the most common causes of data loss and/or unplanned systems downtime over the last 12 months
- Despite the challenges and concerns over data protection, few have fully implemented Zero Trust security

The increasing threat of cyber attacks

- There has been an increase in organizations experiencing a cyberattack or incident in the last 12 months, costing businesses $1.92 million, on average
- Many organizations are concerned that their backup data could become infected or corrupted by ransomware attacks
- Adding to the risk, there is a misguided over-confidence surrounding the consequences of a ransomware attack
- Despite ransomware insurance policies being commonplace, they come heavily caveated, leaving organizations financially vulnerable

The use of multicloud

- Public cloud remains a popular choice when updating existing and deploying new applications, but their are concerns over data security
- Due to security concerns many organizations are moving, or are considering moving, a portion of their workloads on premises from public clouds
- With cyber-related incidents on the rise, and confidence in data protection strategies low, many see security as the most important capability when enabling hybrid, multi-cloud operations

Securing a cloud environment

- Organizations currently use various backup tools and solutions to protect their workloads, but acknowledge upgrades are needed
- Organizations are becoming increasingly reliant on cloud service providers to protect their workloads across cloud environments