

Global Data Protection Index

Cyber Resiliency Multicloud Edition

Understanding the impact of cyber threats, multiclouds, GenAI, operational complexity and more

Data protection challenges resulting in disruption are on the rise with public clouds and cyberattacks the leading areas of concern. Organizations that continue to modernize data protection can minimize risk and raise confidence levels as they pursue digital transformation.

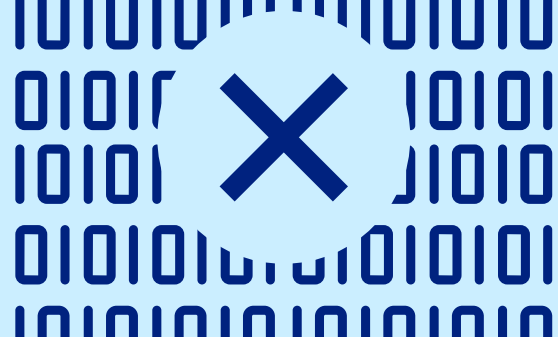
Widespread concerns and a lack of confidence over existing data protection measures are leaving organizations in a vulnerable position

57%

are not very confident in their organization's ability to meet its backup and recovery service level objectives

With 79%

concerned they will experience a disruptive event in the next 12 months



2.59TB

worth of **data has been lost**, on average, in the last 12 months, **costing \$2.40 million**, on average

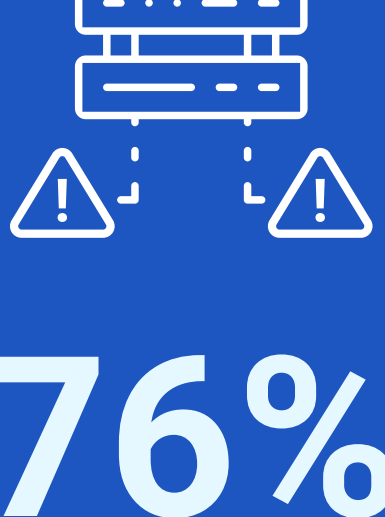


are concerned that their **backup data could become infected or corrupted** even with immutability, sound backup and recovery practices

Cyber-attacks pose an ever present and increasing threat

57%

say that their organization has experienced a cyber-attack or cyber-related incident in the last 12 months. **Costing organizations \$1.68 million**, on average



76%

are concerned that their organization's existing data protection measures are unable to cope with malware and ransomware threats



66%

are not very confident that all business-critical data can be reliably recovered in the event of a destructive cyber-attack



Yet 54%

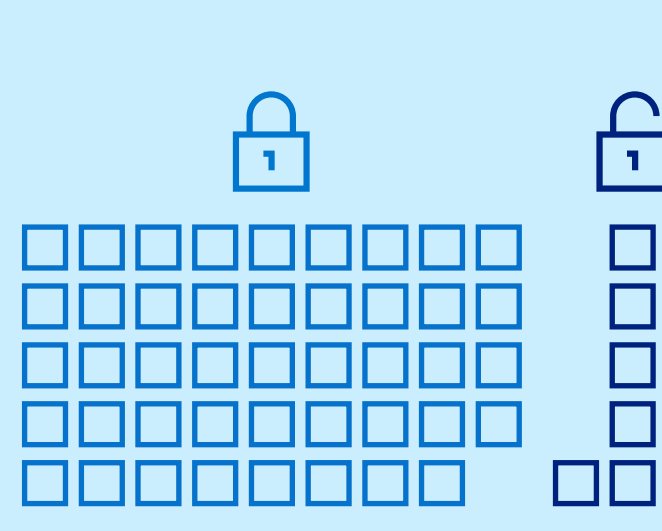
invest more in cyber prevention than cyber recovery despite these concerns

Artificial Intelligence has the potential to increase the cyber resiliency of organizations, but there are concerns over data protection

42% report that their organization is investing in AI technology to better defend against attacks



46% believe **generative AI** can initially provide an **advantage to organizations** defending against cyber criminals



85%

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

Security is a major concern for organizations when using public, multicloud environments

76%

of those using **hybrid or public cloud** when updating or deploying applications are **not very confident** that their **organization can protect all the data** across their public clouds



39% face challenges over **data security** when **maintaining data** in public, multicloud environments

The majority of respondents believe the most important capabilities for enabling hybrid and multicloud operations include the ability to:

59% **Protect multi-workload environments**

55% **Ensure cybersecurity**

Organizations require external support to protect their workloads and ensure backup capabilities



96% of organizations who enlist cloud service providers to protect their workloads report that they have a **separate contract dedicated to this**



63% report that their organization uses **backup and recovery tools** provided by their cloud service provider to some extent



50%

of organizations have brought in outside support, including cyber recovery services to improve cyber resiliency

Dell Technologies delivers cyber recovery, backup, disaster recovery, long-term retention, and more to help you protect all your data and applications.

Learn more about Dell modern, simple, resilient multicloud data protection:



Research carried out by Vanson Bourne between September and October 2023. Respondents were IT and IT security decision makers from both private and public organizations with 250+ employees. There were a total of 1,300 respondents from four regions – 200 from the Americas (US, Mexico and Brazil), 675 from EMEA (UK, France, Germany, Italy, South Africa and UAE), 375 from APJ (Australia, India, Japan, Singapore and South Korea) and 150 from China.

Commissioned by Dell Technologies