DELLTechnologies | VansonBourne

The Data Protection Landscape for K-12 and Higher Education Institutions

Global Data Protection Index 2021 Snapshot

Contents

Introduction

The data protection challenge facing K-12 and Higher Education institutions has never been greater. Data loss and downtime issues are pervasive across the sector, and institutions need to act urgently to prevent further incidents occurring.

However, protecting data is a task growing in magnitude. Education providers must look to solutions which are able to help them cope with the continued growth in the volume of data they are managing, coupled with a rise in cyberthreats and increasing complexity of the IT infrastructure data exists across.
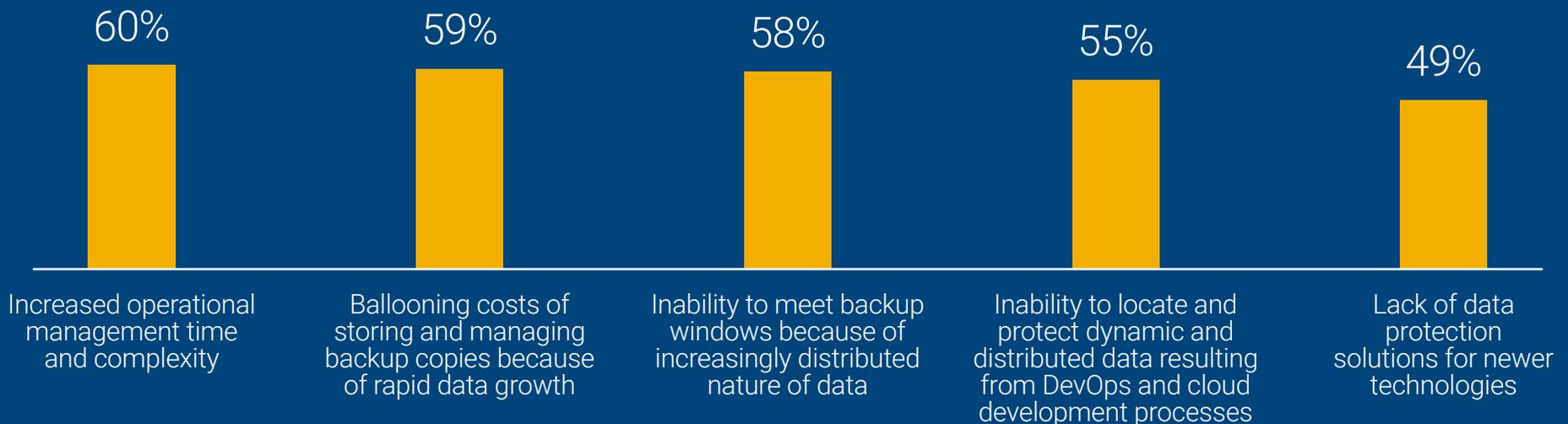
Coping with the unrelenting growth in data

The greater the volume of data an institution has to manage, the more complicated protecting it becomes. And this is a complication which is growing year on year for education providers. The average volume of data these organizations are managing has risen from 11.33 PB in 2019, to 12.26 PB in 2021

With this data including confidential records of staff, students, and their families, as well as boundless learning materials and data to support leadership teams in their strategic decision making, it is paramount that these organizations are able to protect their data.

However, the growth of data has created numerous data protection challenges relating to both its volume and how distributed it has become. Data has become increasingly complex and time consuming to manage (60%) and is costing more and more to store and backup (59%).

Alarmingly, the difficulty of managing increasingly distributed data can also mean that some data is left unprotected – with an inability to meet backup windows (58%) and to locate dynamic and distributed data resulting from DevOps and cloud development processes (55%) being issues for many organizations.

Which of the following challenges is your organization facing in relation to data protection?

| 60%	59%	58%	55%	49%
Increased operational management time and complexity	Ballooning costs of storing and managing backup copies because of rapid data growth	Inability to meet backup windows because of increasingly distributed nature of data	Inability to locate and protect dynamic and distributed data resulting from DevOps and cloud development processes	Lack of data protection solutions for newer technologies

The challenges of protecting these increasing volumes of data mean that many are struggling to implement robust measures to ensure that their data is protected. Almost six in ten (59%) aren't very confident they are meeting their backup and recovery service level objectives (SLOs), which could mean they are at risk of not being able to recover their data quickly or effectively enough in the event of a data loss incident...

The threat to data in 2021

The experience of the past 12 months tells us that education institutions are at high risk of a threat to their data. 88% have experienced at least one disruptive incident which meant they were unable to access their data, indicating that current protection levels are far from satisfactory:
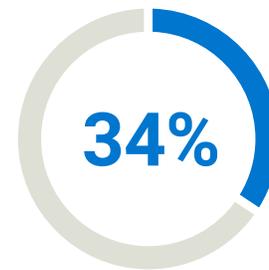
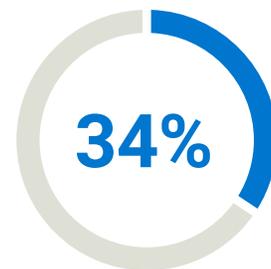## Has your organization suffered from any of the following in the last 12 months?
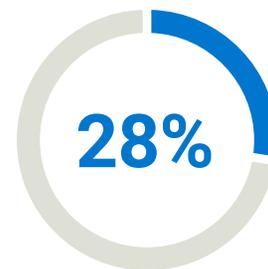
52%
Unplanned systems downtime
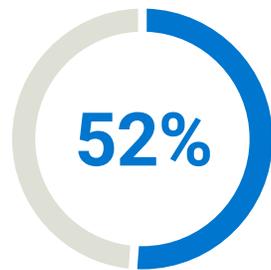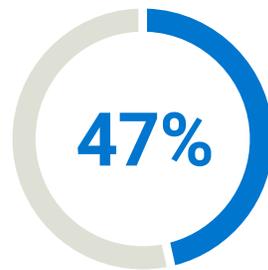
47%
Cyber-attack or other cyber incident that prevented access to data

34%
Data Loss

34%
Local disaster which affected access to data for an entire site or group

28%
Inability to recover data from the current data protection method or product

12%
We have not experienced any of the above

Experiencing these incidents can be hugely damaging for organizations if they aren't able to recover data lost during them – however at present 58% are not very confident that in the event of a data loss incident they can fully recover systems/data to meet service level objectives. On top of this, the financial cost of experiencing a data loss incident or downtime can be enormous:

o   Estimated cost of data loss over the past 12 months: **$908,523**
o   Estimated cost of unplanned systems downtime over the past 12 months: **$454,003**

Organizations in the education sector, with tight budgets and limited resources, could be financially devastated by these costs, making the need for them to ensure they have suitable data protection solutions in place ever more important. In light of these threats, education institutions must take action to improve their protections, and urgently – 71% are concerned that they will suffer a disruptive event in the next 12 months.

The growing cybersecurity threat

Adding further complication to the task of data protection is the rise in cybersecurity threats. Organizations must ensure that their data is protected in the event of a successful cybersecurity attack, however for many this is not currently the case.

Two thirds (67%) of respondents from K-12 and Higher Education institutions are concerned their existing data protection measures may not be sufficient to cope with malware and ransomware threats. Given the confidential nature of much of the data schools and universities are managing, it is critical that they are protected against attacks in which this data could be held hostage by a malicious actor. In addition to these concerns, only 40% are very confident that they could recover all business-critical data in the event of a destructive cyber attack.

The challenge of defending against cybersecurity attacks is one which has become more difficult with the rise in remote learning and work, and endpoints moving out of education institutions and into the homes of students, teachers, and other staff, where they are potentially less protected. 86% state that their organization has increased exposure to data loss from cyber threats with the growth of staff and students working and learning from home.

Remote work and learning is unlikely to go away any time soon, making it essential for organizations to improve their data protection in defence against this increased threat level.

67%
of respondents from K-12 and Higher Education institutions are concerned their existing data protection measures may not be sufficient to cope with malware and ransomware threats.

60%
are not very confident that they could recover all business-critical data in the event of a destructive cyber attack.

86%
state that their organization has increased exposure to data loss from cyber threats with the growth of staff and students working and learning from home.

Moving to the cloud

It is crucial that organizations ensure they can protect their data regardless of where their applications are deployed – for the education sector, public cloud is a popular choice for institutions when they are choosing where to update their existing applications and when deploying new ones.

When updating existing applications or deploying new applications, what direction(s) is your organization taking?

	Private cloud (on-premises)	Private cloud (hosted)	Public cloud (IaaS)	Public cloud (PaaS)	Public cloud (SaaS)	Hybrid cloud
Updating existing applications	44%	41%	47%	35%	38%	22%
Deploying new applications	27%	36%	45%	39%	33%	17%

■ Updating existing applications   ■ Deploying new applications
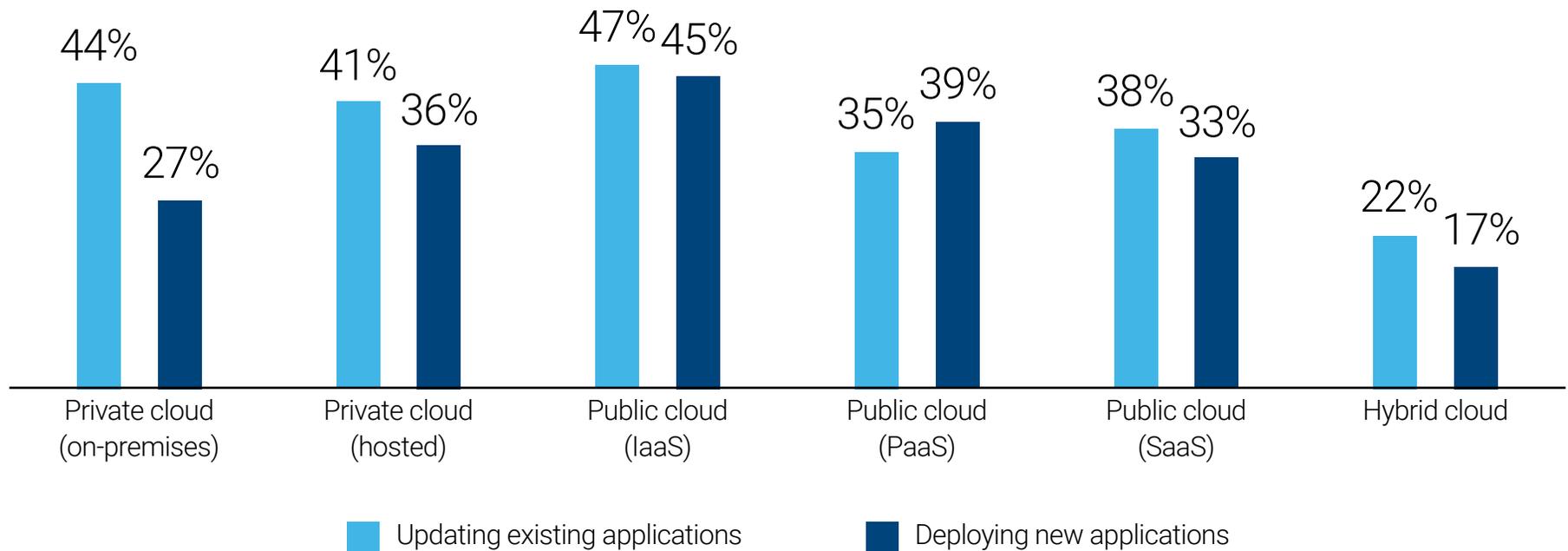
The public cloud is also in widespread use as part of education organizations' data protection strategies. It plays a crucial role in the protection of data created in edge computing locations – 69% using it for this purpose. Further to this, just over two thirds (68%) are utilizing the public cloud for long term retention, and 66% use it for disaster recovery.

While public cloud services can be advantageous when it comes to protecting data, due to the protections the cloud providers themselves have in place, this does not absolve the organization of responsibility for data protection.

Is data in the public cloud protected?

While the public cloud is a popular choice when it comes to deploying and updating applications within the education sector, there are concerns about how well protected data in it is. This is highlighted by the majority (56%) of ITDMs who are not very confident they can protect all data across their public cloud environment. If the move to public cloud environments is not combined with robust data protection measures, organizations could be exposing themselves to even greater vulnerabilities.

Education institutions cannot risk simply assuming that their data is protected just because it is held in a public cloud. A fifth (20%) of those using multiple cloud environments believe that each cloud service provider is responsible for protecting these workloads. Similarly, a quarter (24%) of those who are running virtualized workloads using VMware in the cloud state that their service provider is protecting these workloads.

Yet, only 46% of these organizations have separate contracts with their cloud service providers for the protection of all application workloads. Those who don't have these contracts could be at risk of leaving their data unprotected if they falsely believe their cloud providers are responsible for protecting them.

20%
of those using multiple cloud environments believe that each cloud service provider is responsible for protecting these workloads.

24%
of those who are running virtualized workloads using VMware in the cloud state that their service provider is protecting these workloads.

46%
of these organizations have separate contracts with their cloud service providers for the protection of all application workloads.

The move to as-a-Service

When looking at the data protection landscape for the education sector, the move towards usage of as-a-Service solutions cannot be ignored. Many as-a-Service solutions are being prioritized by organizations in the education sector, with storage-as-a-Service a clear stand out (54%). These solutions can offer organizations new ways to simplify their data protection approach, while providing flexibility and making up for shortages in expertise.
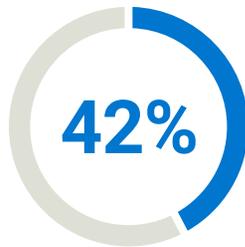
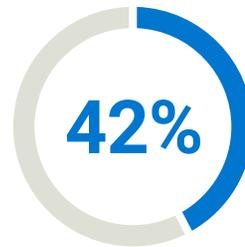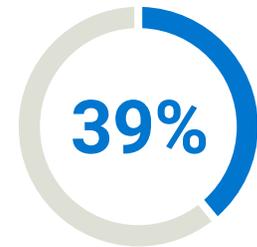## Which as-a-Service offerings are the highest priority for your organization?

54%
Storage-as-a-service

42%
Backup-as-a-service

42%
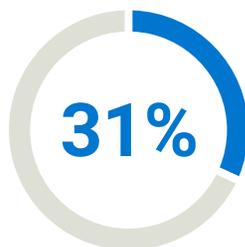Compute-as-a-service

39%
Disaster recovery-as-a-service
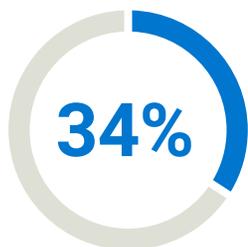
34%
Networking-as-a-service

31%
Cyber-recovery-as-a-service

26%
AI-as-a-service
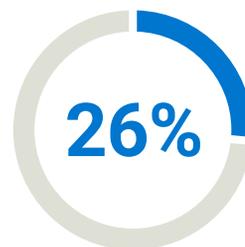
21%
Edge-as-a-service

In addition, the majority

(87%) of surveyed IT decision makers within the education sector say their organization would be more likely to use a vendor that has multiple as-a-Service solutions, indicating a desire to consolidate the number of vendors they are using to provide data protection services.

Moving towards as-a-Service solutions could offer numerous benefits due to their convenience and scalability – however institutions need to assess whether all the solutions available are able to deliver the right level of protection for education data.

Conclusion

The data protection challenge facing K-12 and Higher Education institutions has never been greater. The growth in the volume of data that organizations are dealing with is something that has subsequently increased the challenge of protecting it.

There are signs that many are struggling to cope with this challenge. Incidents which have threatened organizations' access to their data are widespread across the sector, and such incidents can have hugely damaging impacts. There is an urgent need for institutions within the education sector to improve the data protection solution(s) they are currently using to address this.

However, there are concerns that current data protection solutions are not adequate to protect against sophisticated malware and ransomware attacks. These solutions must also protect against the other challenges organizations are facing – including the rise in cybersecurity attacks and the need to protect data across public cloud environments.

How Dell Technologies Can Help

DELLTechnologies

Dell Technologies is #1 in Data Protection Appliances & Software[1] and has a strong footprint in the education space, with over 14,000 colleges and university campuses and 300,000 K-12 classrooms worldwide leveraging its solutions. Dell Technologies also provides tailored support to their education customers with Higher Education and K-12 Strategists that have extensive backgrounds in implementation of learning technology for institutions of all sizes.

Dell Technologies can help K-12 and Higher Education organizations deploy cost-effective data management and protection solutions and deliver greater efficiency, predictability, and organizational agility.

- Innovative data protection solutions with proven and agile cloud data backup solutions for private, hybrid and multi-cloud environments.
- Powerful, automated data protection for VMware hybrid cloud environments and Tanzu modern applications that simplifies administration and lowers TCO.
- Protect critical data, identify suspicious activity and perform data recovery with easy-to-deploy cyber recovery management and automation software.

Dell Technologies Data Protection Solutions
Learn more at delltechnologies.com/dataprotection

Dell Technologies Education Solutions
In Higher Education – Learn more at delltechnologies.com/hied
In K-12 – Learn more at delltechnologies.com/k12

[1] Based on combined revenue from the IDC 2Q21 Purpose-Built Backup Appliance (PBBA) Tracker, with select Storage Software segments from the 2Q21 Storage Software and Cloud Services Qview.

About Vanson Bourne
Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.