Global Data Protection
Index 2021

Key Findings – July 2021
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 correlates 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

Not very confident that systems/data can be fully recovered in order to meet business service level objectives in the event of a data loss incident

67% 64% 65%

2018 total 2019 total 2021 total
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.

- **Average cost of data loss in the last 12 months (in USD):** $959,493
- **Average cost of unplanned systems downtime in the last 12 months (in USD):** $513,067
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.

Not very confident that all business critical data can be recovered in the event of a destructive cyber attack

- 2018 total: 65%
- 2019 total: 69%
- 2021 total: 67%
3. Keeping pace with new and emerging technologies
Organizations are investing in many new technologies, which could be complicating their data protection challenges

- SaaS applications (e.g., O365, Salesforce) - 63%
- Cloud native applications - 59%
- Artificial intelligence/machine learning - 53%
- Edge Cloud (enables the consumption and operation of infrastructure in Edge locations via an as-a-Service model) - 49%
- Edge/LoT devices - 38%
- Containers - 29%
And it is the case that many organizations are struggling to protect these technologies.

- Edge Cloud (enables the consumption and operation of infrastructure in Edge locations via an as-a-Service model): 68%
- Cloud native applications: 67%
- Artificial intelligence/machine learning: 67%
- Edge/IoT devices: 66%
- SaaS applications (e.g., O365, Salesforce): 58%
- Containers: 53%
The difficulty of protecting new and emerging technologies is likely contributing to poor confidence that data protection solutions are future-ready.

Our data protection solutions won't be able to meet all future business challenges:

- 2018 total: 84%
- 2019 total: 81%
- 2021 total: 82%
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

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
  - 57%
- Uses multiple data protection vendors
  - 64%
- 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

<table>
<thead>
<tr>
<th>Updating existing applications</th>
<th>Deploying new applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private cloud (on-premises)</td>
<td>Private cloud (on-premises)</td>
</tr>
<tr>
<td>41%</td>
<td>29%</td>
</tr>
<tr>
<td>Private cloud (hosted)</td>
<td>Private cloud (hosted)</td>
</tr>
<tr>
<td>43%</td>
<td>37%</td>
</tr>
<tr>
<td>Public cloud (IaaS)</td>
<td>Public cloud (IaaS)</td>
</tr>
<tr>
<td>46%</td>
<td>40%</td>
</tr>
<tr>
<td>Public cloud (PaaS)</td>
<td>Public cloud (PaaS)</td>
</tr>
<tr>
<td>31%</td>
<td>35%</td>
</tr>
<tr>
<td>Public cloud (SaaS)</td>
<td>Public cloud (SaaS)</td>
</tr>
<tr>
<td>35%</td>
<td>30%</td>
</tr>
<tr>
<td>Hybrid cloud</td>
<td>Hybrid cloud</td>
</tr>
<tr>
<td>18%</td>
<td>15%</td>
</tr>
</tbody>
</table>
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

Disaster recovery

- Yes, we use the public cloud for this currently: 59%
- No, but we plan to use the public cloud for this in the future: 26%
- No, and we do not plan to use the public cloud for this: 13%
- Don’t know: 2%

Long-term retention

- Yes, we use the public cloud for this currently: 60%
- No, but we plan to use the public cloud for this in the future: 26%
- No, and we do not plan to use the public cloud for this: 12%
- Don’t know: 2%
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
- 27% plan to upgrade their data protection solution to enable the backup of workloads across multiple clouds
- 23% use multiple backup tools to protect workloads running in multiple clouds
- 23% use multiple backup tools to protect workloads running in multiple clouds
- 21% believe each cloud service provider is responsible for protecting their workloads
- 6% believe our current backup solution allows us to protect workloads running in multiple clouds
- 0% believe we use multiple backup tools to protect workloads running in multiple clouds
- 21% believe we are not running workloads in multiple cloud environments
- 0% believe we are not running workloads in multiple cloud environments

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
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.

- Storage-as-a-Service: 47%
- Backup-as-a-Service: 43%
- Disaster Recovery-as-a-Service: 41%
- Networking-as-a-Service: 37%
- Cyber-Recovery-as-a-Service: 35%
- Compute-as-a-Service: 32%
- AI-as-a-Service: 29%
- Edge-as-a-Service: 23%

No as-a-Service offerings are high priority for my organization: 4%
The popularity of as-a-Service offerings often stems from their flexibility

Reasons for pursuing an as-a-Service offering

- The business requires more flexibility while still maintaining optimal IT operations: 74%
- Need to tactically address bursting: 67%
- Need to shift from CapEx to OpEx: 53%
- Lack of expertise in area to manage ourselves: 49%
- Not enough staff to maintain services ourselves: 47%
- We wouldn't pursue an as-a-Service offering: 3%
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.

<table>
<thead>
<tr>
<th>Event</th>
<th>Total</th>
<th>Use Single Data Protection Vendor</th>
<th>Use Multiple Data Protection Vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unplanned systems downtime</td>
<td>45%</td>
<td>38%</td>
<td>46%</td>
</tr>
<tr>
<td>Cyber attack or other cyber incident that prevented access to data</td>
<td>37%</td>
<td>22%</td>
<td>41%</td>
</tr>
<tr>
<td>Data loss</td>
<td>31%</td>
<td>21%</td>
<td>33%</td>
</tr>
<tr>
<td>Local disaster which affected access to data for an entire site or group</td>
<td>27%</td>
<td>15%</td>
<td>30%</td>
</tr>
<tr>
<td>Inability to recover data from the current data protection method or product</td>
<td>25%</td>
<td>14%</td>
<td>28%</td>
</tr>
<tr>
<td>We have not experienced any of the above</td>
<td>24%</td>
<td>20%</td>
<td>35%</td>
</tr>
</tbody>
</table>
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