Global Data Protection Index – Cloud Environments

Key Findings – March 2020
Demographics – who did we interview?

1,000 IT decision makers were interviewed in November and December 2019

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)
Focus of key findings:

1. The rise of disruption
2. Hybrid cloud – the new normal
3. VMware data protection
4. Cloud data protection vulnerability
5. Data protection for newer technologies
6. Increased risk of using multiple data protection vendors
1. The rise of disruption
Disruptive events are on the rise, with even more organizations falling victim to one in 2019 compared to 2018.

<table>
<thead>
<tr>
<th>Event</th>
<th>Total 2018</th>
<th>Total 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unplanned systems downtime</td>
<td>41%</td>
<td>45%</td>
</tr>
<tr>
<td>Cyber-attack or other cyber incident that prevented access to data</td>
<td>28%</td>
<td>35%</td>
</tr>
<tr>
<td>Data loss</td>
<td>28%</td>
<td>35%</td>
</tr>
<tr>
<td>Inability to recover data from the current data protection method or product</td>
<td>27%</td>
<td>27%</td>
</tr>
<tr>
<td>Local disaster which affected access to data for an entire site or group</td>
<td>25%</td>
<td>23%</td>
</tr>
<tr>
<td>We have not experienced any</td>
<td>24%</td>
<td>18%</td>
</tr>
</tbody>
</table>

Have **suffered from a disruptive event** (e.g. downtime or data loss) in the last 12 months, compared to **76%** in 2018.
Looking beyond the financial damage, disruption also results in a wide range of other consequences for organizations.

- Loss of employee productivity: 47%
- Delay in product or service development: 46%
- Inability to provide essential services: 44%
- Loss of revenue: 43%
- Loss of customer loyalty: 41%
- Delay in time to market: 36%
- Loss of a new business opportunity: 30%
- Loss of business to a competitor: 27%
- Loss of customers: 27%
- Loss of repeat business: 24%
- Punitive fines: 18%
There is also a considerable lack of confidence in a number of crucial areas relating to the data protection that organizations currently have in place.

There is a lack of confidence in terms of:

- Reliably recovering all business-critical data in the event of a cyberattack: 69%
- Fully recovering systems/data from all platforms in the event of a data loss incident: 64%
- Compliance with regional data governance regulations: 62%
- Meeting backup and recovery service level objectives: 62%
Meanwhile, there is widespread concern that more disruption will be experienced over the next 12 months

*The majority (68%) of respondents are concerned that their organization will experience a disruptive event in the next 12 months* (such as unplanned systems downtime)
Further adding to the challenge of disruption is the growing amount of data that organizations are managing – between 2018 and 2019, data volumes have increased by 39%.

Average volume of data being managed (in PB)

- Average 2016: 1.45 PB
- Average 2018: 9.70 PB
- Average 2019: 13.53 PB
Unexpected downtime to critical applications can take significant time to recover from too – 8 hours on average in 2019

8 hours is the average recovery time should an unexpected event cause downtime to critical applications

(2018 = 7 hrs, 2016 = 7 hrs)
The cost of downtime is also on the up in organizations. Between 2018 and 2019 this increased by 54%, on average.

**Estimated total cost of downtime in the last 12 months**
(average, in USD)

$526,845  
In 2018

$810,018  
In 2019

54%  
Increase in the average cost of downtime between 2018 and 2019
2. Hybrid cloud – the new normal
Most organizations are deploying mission-critical workloads into both public and private clouds.

### Public cloud

<table>
<thead>
<tr>
<th>Category</th>
<th>Planning to run in the public cloud in the future</th>
<th>Running in the public cloud currently</th>
</tr>
</thead>
<tbody>
<tr>
<td>Productivity (e.g. Office 365)</td>
<td>95%</td>
<td>39%</td>
</tr>
<tr>
<td>CRM</td>
<td>90%</td>
<td>44%</td>
</tr>
<tr>
<td>Archiving</td>
<td>89%</td>
<td>46%</td>
</tr>
<tr>
<td>Content management systems</td>
<td>89%</td>
<td>46%</td>
</tr>
<tr>
<td>Data warehouse</td>
<td>88%</td>
<td>47%</td>
</tr>
<tr>
<td>ERP</td>
<td>88%</td>
<td>49%</td>
</tr>
<tr>
<td>BI/analytics systems</td>
<td></td>
<td>53%</td>
</tr>
</tbody>
</table>

### Private cloud

<table>
<thead>
<tr>
<th>Category</th>
<th>Planning to run in the private cloud in the future</th>
<th>Running in the private cloud currently</th>
</tr>
</thead>
<tbody>
<tr>
<td>Productivity (e.g. Office 365)</td>
<td>88%</td>
<td>36%</td>
</tr>
<tr>
<td>CRM</td>
<td>86%</td>
<td>41%</td>
</tr>
<tr>
<td>Archiving</td>
<td>86%</td>
<td>41%</td>
</tr>
<tr>
<td>Content management systems</td>
<td>85%</td>
<td>46%</td>
</tr>
<tr>
<td>Data warehouse</td>
<td>85%</td>
<td>37%</td>
</tr>
<tr>
<td>ERP</td>
<td>85%</td>
<td>43%</td>
</tr>
<tr>
<td>BI/analytics systems</td>
<td></td>
<td>46%</td>
</tr>
</tbody>
</table>

[Image of bar charts showing percentages for public and private cloud deployment by category]
3. VMware data protection
For many, the hybrid cloud approach for application deployments will be based on VMware infrastructure. However, there is no clear standout in terms of how organizations are protecting VMware workloads in the cloud.

- 27%: We plan to upgrade our data protection solution to enable hybrid cloud backup of VMware workloads
- 23%: Our cloud service provider is responsible for protecting our workloads
- 23%: With backup tools available in the cloud service provider marketplace
- 21%: With backup tools that we currently use and operate on-premise
- 5%: We are not running or planning to run VMware workloads in the cloud
- 1%: Don't know
4. Cloud data protection vulnerability
When deploying new applications, most organizations favour a cloud-based deployment model

Choose cloud deployments (public, private and/or hybrid) for new applications
The decision to use public cloud when deploying new business applications is driven by a range of important business benefits:

- Better performance: 61%
- Improved security: 59%
- More reliable data protection: 56%
- Enhanced scalability: 44%
- Lower costs: 44%
- Faster time-to-market: 37%

Say the decision to use public cloud when deploying new business applications is driven by more reliable data protection.
For those running workloads in multiple cloud environments, there is not a clear “go to” in terms of protection

20% Believe that responsibility for protecting workloads running in multiple clouds sits with the cloud service providers themselves

- 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
- We plan to upgrade our data protection solution to enable the backup of workloads across multiple clouds
- Each cloud service provider is responsible for protecting our workloads
- We are not running workloads in multiple cloud environments
However, most of those that say their cloud service provider protects their cloud-based workloads do not actually have separate contracts for protection of all workloads.
5. Data protection for newer technologies
For the vast majority of organizations, their current data protection solution(s) will not be sufficient for meeting all future business challenges.

- Our current data protection solutions will not be able to meet any future business challenges: 7% (Total 2018), 3% (Total 2019)
- Our current data protection solutions will be able to meet a minority of future business challenges: 31% (Total 2018), 27% (Total 2019)
- Our current data protection solutions will be able to meet the majority of future business challenges: 46% (Total 2018), 50% (Total 2019)
- Our current data protection solutions will be able to meet all future business challenges: 16% (Total 2018), 20% (Total 2019)

Say that their organization's existing data protection solution(s) will not be able to meet all future business challenges.
Almost all organizations are making at least some investment into newer or emerging technologies

- Cloud-native applications (e.g. Cloudera, Hadoop): 58%
- Artificial intelligence/machine learning: 53%
- SaaS applications: 51%
- 5G/Cloud Edge (infrastructure): 49%
- IoT/End Point: 36%
- Chatbots/virtual assistants: 35%
- Robotic process automation: 32%
- Containers: 25%
- We are not investing in any: 2%

98% are investing in at least one newer/emerging technology.
Around half or more of those using each of the technologies listed are struggling to find suitable data protection for them.
Despite their obvious value, emerging technologies are widely recognized as introducing additional challenges and concerns:

- **52%** consider the lack of data protection for newer technologies to be one of the top five data protection challenges facing their organization.

- **71%** agree that emerging technologies create more complexity when it comes to data protection.

- **61%** agree that emerging technologies pose a risk to data protection.

- **62%** agree that their organization’s existing data protection measures may not be sufficient to cope with new and emerging technologies.
6. Increased risk of using multiple data protection vendors
Organizations are increasingly using multiple data protection vendors for their data protection needs – in 2019, 80% of organizations are doing this.

We use more than one vendor

- Total 2016: 60%
- Total 2018: 76%
- Total 2019: 80%
Those using multiple data protection vendors are more likely to report suffering from disruption over the last 12 months.
For organizations that have experienced data loss in the last 12 months, the costs are typically nearly 5x higher for those using multiple vendors, on average.

Estimated total cost of data loss in the last 12 months (average, in USD)

$1,090,436
Use multiple data protection vendors

$227,781
Use single data protection vendor

5x
Higher average cost from data loss experienced by those using multiple vendors
For those that have experienced unplanned downtime in the last 12 months, the costs are typically nearly 2x higher for those using multiple vendors, on average.

**Estimated total cost of downtime in the last 12 months (average, in USD)**

$881,207
Use multiple data protection vendors

$473,512
Use single data protection vendor

Higher average cost from unplanned downtime experienced by those using multiple vendors.
The rise of disruption

- Disruptive events are on the rise, with even more organizations falling victim to one in 2019 compared to 2018
- Looking beyond the financial damage, disruption also results in a wide range of other consequences for organizations
- There is also a considerable lack of confidence in a number of crucial areas relating to the data protection that organizations currently have in place
- Meanwhile, there is widespread concern that more disruption will be experienced over the next 12 months
- Further adding to the challenge of disruption is the growing amount of data that organizations are managing – between 2018 and 2019, data volumes have increased by 39%
- Unexpected downtime to critical applications can take significant time to recover from too – 8 hours on average in 2019
- The cost of downtime is also on the up in organizations. Between 2018 and 2019 this increased by 54%

Hybrid cloud – the new normal

- Most organizations are deploying mission-critical workloads into both public and private clouds

VMware data protection

- For many, the hybrid cloud approach for application deployments will be based on VMware infrastructure. However, there is no clear standout in terms of how organizations are protecting VMware workloads in the cloud
Key Findings - In Summary (2/2)

Cloud data protection vulnerability

• When deploying new applications, most organizations favour a cloud-based deployment model
• The decision to use public cloud when deploying new business applications is driven by a range of important business benefits
• For those running workloads in multiple cloud environments, there is not a clear “go to” in terms of protection
• However, most of those that say their cloud service provider protects their cloud-based workloads do not actually have separate contracts for protection of all workloads

Data protection for newer technologies

• For the vast majority of organizations, their current data protection solution(s) will not be sufficient for meeting all future business challenges
• Almost all organizations are making at least some investment into newer or emerging technologies
• Around half or more of those using each of the technologies listed are struggling to find suitable data protection for them
• Despite their obvious value, emerging technologies are widely recognized as introducing additional challenges and concerns

Increased risk of using multiple data protection vendors

• Organizations are increasingly using multiple data protection vendors for their data protection needs – in 2019, 80% of organizations are doing this
• Those using multiple data protection vendors are more likely to report suffering from disruption over the last 12 months
• For organizations that have experienced data loss in the last 12 months, the costs are typically nearly 5x higher for those using multiple vendors, on average
• For those that have experienced unplanned downtime in the last 12 months, the costs are typically nearly 2x higher for those using multiple vendors, on average