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.

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>60%</td>
<td>Not very confident that their organization is meeting its backup and recovery service level objectives (SLOs)</td>
</tr>
<tr>
<td>79%</td>
<td>Concerned that they will experience a disruptive event in the next twelve months</td>
</tr>
<tr>
<td>75%</td>
<td>Concerned their organization's existing data protection measures may not be sufficient to cope with malware and ransomware threats</td>
</tr>
<tr>
<td>65%</td>
<td>Not very confident that their organization could fully recover systems/data from all platforms in the event of a data loss incident</td>
</tr>
</tbody>
</table>
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

- **Cyber-attack or other cyber incident that prevented access to data**
  - 2018 (n=2,200): 28%
  - 2019 (n=1,000): 35%
  - 2020 (n=1,000): 48%
  - 2021 (n=1,000): 52%
  - 2022 (n=1,000): 40%
- **Local disaster which affected access to data for an entire site or group**
  - 2018 (n=2,200): 25%
  - 2019 (n=1,000): 23%
  - 2020 (n=1,000): 27%
  - 2021 (n=1,000): 35%
  - 2022 (n=1,000): 31%
  - 2023 (ITDMs only) (n=1,000): 29%
- **Inability to recover data from the current data protection method or product**
  - 2018 (n=2,200): 27%
  - 2019 (n=1,000): 27%
  - 2020 (n=1,000): 25%
  - 2021 (n=1,000): 40%
  - 2022 (n=1,000): 41%
- **Unplanned systems downtime**
  - 2018 (n=2,200): 41%
  - 2019 (n=1,000): 45%
  - 2020 (n=1,000): 45%
  - 2021 (n=1,000): 36%
  - 2022 (n=1,000): 40%
- **Data loss**
  - 2018 (n=2,200): 28%
  - 2019 (n=1,000): 35%
  - 2020 (n=1,000): 27%
  - 2021 (n=1,000): 27%
  - 2022 (n=1,000): 24%
- **We have not experienced any of the above**
  - 2018 (n=2,200): 18%
  - 2019 (n=1,000): 24%
  - 2020 (n=1,000): 24%
  - 2021 (n=1,000): 14%
  - 2022 (n=1,000): 10%
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:

- Unplanned systems downtime:
  - Total (n=1,500): 38%, 42%
  - Americas (n=300): 37%, 40%
  - EMEA (n=675): 29%
  - APJ (excl. China) (n=375): 27%
  - China (n=150): 23%

- Data loss:
  - Total (n=1,500): 28%, 31%
  - Americas (n=300): 26%
  - EMEA (n=675): 23%
  - APJ (excl. China) (n=375): 27%
  - China (n=150): 22%

In the last 12 months:
- 26 hours on average 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.

Copyright © Dell Inc. All Rights Reserved.
External security threats are the most common causes of data loss and/or unplanned systems downtime over the last 12 months.

<table>
<thead>
<tr>
<th>Cause of data loss and/or systems downtime in the last 12 months</th>
<th>Total (n=834)</th>
<th>Americas (n=172)</th>
<th>EMEA (n=377)</th>
<th>APJ (excl. China) (n=217)</th>
<th>China (n=68)</th>
</tr>
</thead>
<tbody>
<tr>
<td>External security breach (e.g. malware, spyware, viruses, botnets, ransomware or cyber-terrorism or attack)</td>
<td>45%</td>
<td>40%</td>
<td>33%</td>
<td>31%</td>
<td>40%</td>
</tr>
<tr>
<td>Software failure</td>
<td>34%</td>
<td>34%</td>
<td>33%</td>
<td>33%</td>
<td>33%</td>
</tr>
<tr>
<td>Hardware failure</td>
<td>35%</td>
<td>30%</td>
<td>32%</td>
<td>31%</td>
<td>33%</td>
</tr>
<tr>
<td>Data corruption</td>
<td>33%</td>
<td>31%</td>
<td>33%</td>
<td>33%</td>
<td>30%</td>
</tr>
<tr>
<td>Service/cloud provider internal security breach (e.g. internal employee)</td>
<td>29%</td>
<td>18%</td>
<td>20%</td>
<td>19%</td>
<td>26%</td>
</tr>
<tr>
<td>Internal security breach (e.g. internal employee)</td>
<td>30%</td>
<td>27%</td>
<td>26%</td>
<td>26%</td>
<td>23%</td>
</tr>
<tr>
<td>Loss of power</td>
<td>29%</td>
<td>24%</td>
<td>23%</td>
<td>24%</td>
<td>29%</td>
</tr>
<tr>
<td>Physical security (e.g. loss/theft of equipment)</td>
<td>26%</td>
<td>23%</td>
<td>23%</td>
<td>23%</td>
<td>23%</td>
</tr>
<tr>
<td>User error</td>
<td>26%</td>
<td>29%</td>
<td>26%</td>
<td>25%</td>
<td>29%</td>
</tr>
<tr>
<td>Deliberate employee sabotage</td>
<td>20%</td>
<td>21%</td>
<td>20%</td>
<td>21%</td>
<td>25%</td>
</tr>
<tr>
<td>Natural disaster (e.g. tsunami, hurricane, earthquake, flood, fire)</td>
<td>27%</td>
<td>18%</td>
<td>16%</td>
<td>16%</td>
<td>20%</td>
</tr>
</tbody>
</table>

Total (n=834) | Americas (n=172) | EMEA (n=377) | APJ (excl. China) (n=217) | China (n=68)
Despite the challenges and concerns over data protection, few have fully implemented Zero Trust security.

### Organizations' journey to implementing Zero Trust security

- **My organization does not yet have an understanding of Zero Trust**: 7%
- **My organization is just now discussing what Zero Trust means to our operations**: 19%
- **My organization understands and is committed to implementing Zero Trust practices**: 23%
- **My organization is in the planning phase of implementing a Zero Trust security architecture**: 20%
- **My organization is actively deploying Zero Trust security architecture capabilities**: 21%
- **My organization has fully implemented a Zero Trust security architecture and its ongoing maintenance**: 8%

*Filter: Data Split: Region = Total (n=1 500)*
2. The increasing threat of cyberattacks
Concerns over data protection measures are widespread, and with confidence lacking, organizations find themselves in a vulnerable position.

Not "very confident" that all business-critical data can be reliably recovered in the event of a destructive cyberattack, split by year:

- **2018 (n=2,200)**: 65%
- **2019 (n=1,000)**: 69%
- **2021 (n=1,000)**: 67%
- **2022 (n=1,000)**: 63%
- **2023 (ITDMs only) (n=1,000)**: 69%

Summary: Combination of "Not at all confident", "Not very confident", "Some doubt" and "Moderately confident"

- **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.

Conditions of organization's ransomware insurance policy

- My organization must prove 'best practice' cyberthreat prevention activity: 57%
- The policy has a limit on how much they will pay for a claim: 43%
- There are particular scenarios which would make the policy void: 40%
- The policy will not pay out as payment to some entities may be restricted by law: 40%

93% of organizations have a ransomware policy.
Despite many having ransomware policies in place, organizations still find themselves financially vulnerable.

<table>
<thead>
<tr>
<th>Was a ransom paid to gain access to your organization's data, split by region</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, and my organization's ransomware insurance policy paid out fully to cover the ransom</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>36%</td>
</tr>
<tr>
<td>27%</td>
</tr>
<tr>
<td>27%</td>
</tr>
<tr>
<td>3%</td>
</tr>
<tr>
<td>39%</td>
</tr>
</tbody>
</table>

Total (n=819) | Americas (n=169) | EMEA (n=365) | APJ (excl. China) (n=215) | China (n=70)

$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

Steps organizations are taking to improve their cyber resiliency, split by region

- We have brought in outside support including professional services, managed detection and response services, cyber recovery services that come from a partner of our organization
- We do regular cyber recovery testing to ensure systems and processes are in place and operating
- We use machine learning and analytics to help ensure backup data is "clean" before recovering
- We are investing in AI technology to better defend against attacks
- We are using a cyber vault with physical and logical separation of data from the production environment
- We follow a specific security framework such as NIST or Zero Trust
- We are ensuring our backup data is immutable

Total (n=1 500)  Americas (n=300)  EMEA (n=675)  APJ (excl. China) (n=375)  China (n=150)
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.

Impact of generative AI on cyber threats and data security, split by region:

- It will initially provide an advantage to cyber criminals and increase the threat of cyberattacks:
  - Total (n=1500) 27%
  - Americas (n=300) 28%
  - EMEA (n=675) 33%
  - APJ (excl. China) (n=375) 9%
  - China (n=150) 0%

- It will initially provide an advantage to organizations defending against cyber criminals, strengthening their cyber security posture:
  - Total (n=1500) 52%
  - Americas (n=300) 53%
  - EMEA (n=675) 53%
  - APJ (excl. China) (n=375) 46%
  - China (n=150) 20%

- It will both increase the threat of cyberattacks and also strengthen organizations’ cyber security posture which could offset each other:
  - Total (n=1500) 63%
  - Americas (n=300) 21%
  - EMEA (n=675) 19%
  - APJ (excl. China) (n=375) 19%
  - China (n=150) 28%
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.

<table>
<thead>
<tr>
<th>Service Type</th>
<th>2021 (n=1 000)</th>
<th>2022 (n=1 000)</th>
<th>2023 (ITDMs only) (n=1 000)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public cloud (IaaS)</td>
<td>46%</td>
<td>50%</td>
<td>55%</td>
</tr>
<tr>
<td>Public cloud (PaaS)</td>
<td>31%</td>
<td>43%</td>
<td>45%</td>
</tr>
<tr>
<td>Public cloud (SaaS)</td>
<td>35%</td>
<td>37%</td>
<td>37%</td>
</tr>
<tr>
<td>Private cloud (on-premises)</td>
<td>41%</td>
<td>37%</td>
<td>33%</td>
</tr>
<tr>
<td>Private cloud (hosted)</td>
<td>43%</td>
<td>37%</td>
<td>33%</td>
</tr>
<tr>
<td>Hybrid cloud (mix of two or more locations)</td>
<td>18%</td>
<td>22%</td>
<td>20%</td>
</tr>
</tbody>
</table>
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. The report mentions that:

- The complexities of managing multiple public clouds (e.g., multiple tools) affect 44% of organizations.
- The cost of managing multiple public clouds (e.g., administrator overhead) impacts 42% of organizations.
- Concerns over data security (e.g., network latency, interoperability) are a challenge for 40% of organizations.
- Difficulties with accessibility affect 38% of organizations.
- Lack of expertise in the business to manage it affects 35% of organizations.
- Data transfer costs (e.g., egress fees) are a concern for 34% of organizations.
- The amount of downtime experienced is a challenge for 29% of organizations.
- Compliance issues are faced by 26% of organizations.

The data is based on a survey of 1,500 organizations.
Due to security concerns many organizations are moving, or are considering moving, a portion of their workloads on premises from public clouds.

The extent at which organizations are moving workloads on premises from public cloud

- We are considering moving at least some of our workloads on premises from public cloud due to security concerns: 23%
- We are considering moving just our mission critical workloads on premises from public cloud due to security concerns: 35%
- We have/are in the process of moving at least some of our workloads on premises from public cloud due to security concerns: 23%
- We have/are in the process of moving just our mission critical workloads on premises from public cloud due to security concerns: 12%
- We are not considering or moving any workloads on premises from public cloud due to security concerns: 5%

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.
4. Securing a cloud environment
Organizations currently use various backup tools and solutions to protect their workloads, but the need for upgrades are noted.

<table>
<thead>
<tr>
<th>Survey Question</th>
<th>2019 (n=1 000)</th>
<th>2021 (n=1 000)</th>
<th>2022 (n=1 000)</th>
<th>2023 (ITDMs only) (n=1 000)</th>
</tr>
</thead>
<tbody>
<tr>
<td>We use multiple backup tools to protect workloads running in multiple clouds</td>
<td>26%</td>
<td>26%</td>
<td>26%</td>
<td>26%</td>
</tr>
<tr>
<td>Our current backup solution allows us to protect workloads running in multiple clouds</td>
<td>23%</td>
<td>23%</td>
<td>23%</td>
<td>23%</td>
</tr>
<tr>
<td>Each cloud service provider is responsible for protecting our workloads</td>
<td>20%</td>
<td>21%</td>
<td>19%</td>
<td>18%</td>
</tr>
<tr>
<td>We plan to upgrade our data protection solution to enable the backup of workloads across multiple clouds</td>
<td>22%</td>
<td>27%</td>
<td>22%</td>
<td>14%</td>
</tr>
<tr>
<td>We are not running workloads in multiple cloud environments</td>
<td>6%</td>
<td>6%</td>
<td>2%</td>
<td>2%</td>
</tr>
</tbody>
</table>
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

- Yes, for all workloads: 24%
- Yes, for most workloads: 59%
- Yes, but only for some workloads: 12%
- No: 3%

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

Backup and recovery tools supplied by cloud service provider

- My organization always uses tools provided by our cloud service provider (CSP): 26%
- My organization always uses our own software defined tools running in the public cloud: 38%
- My organization uses a mix of the tools provided by our cloud service provider (CSP) and our own software defined tools: 34%
- My organization does not use cloud service provider(s): 1%

Filter: Data Split: Region = Total  
Filter: Data Split: Region = Total
Key findings
- in summary

The data protection risk landscape
- Concerns over data protection measures are widespread, and with confidence 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 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 there 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