ARE YOU PROTECTED?

GET AHEAD OF THE CURVE

DELL EMC – GLOBAL DATA PROTECTION INDEX 2018
INTERVIEWED
2,200
IT DECISION-MAKERS
IN 3 REGIONS:

- 500 Americas
- 1,100 Europe, Middle East, and Africa
- 600 Asia Pacific Japan

18 COUNTRIES
ORGS OF 250 OR MORE EMPLOYEES
BOTH PUBLIC AND PRIVATE ORGS

INDEPENDENT RESEARCH AND ANALYSIS: VANSON BOURNE
MATURITY CURVE
Around one in ten organizations are considered to be data protection leaders in 2018 (compared to 2% in 2016).
Maturity index

Points awarded based on the maturity of their data protection strategy

More points awarded for:
- Shorter recovery times
- Confidence in backup infrastructure
- Modern backup systems
- Higher valuation of data

Maturity scored between 1–138 points*

* Exact scoring included in appendix – questions show points used for the model with a maximum score of 138.
The profile characteristics for each of the following maturity groups tend to be...

**Laggards**
- 2%
- Place little or no value on data
- Have DP solutions that will not meet future challenges
- No consideration of public cloud for DP
- Recovery times often over 12 hours
- Little or no confidence in terms of DP compliance, meeting SLOs, and recovering data in the event of data loss

**Evaluators**
- 29%
- See the potential value of data
- Have DP solutions that will meet a minority of future challenges
- Minimal use of public cloud for DP
- Recovery times 3-9 hours
- Several doubts in terms of DP compliance, meeting SLOs, and recovering data in the event of data loss

**Adopters**
- 57%
- Starting to invest in tools to monetize data
- Have DP solutions that will meet most future challenges
- Use of public cloud for DP
- Recovery times 2-6 hours
- Moderate confidence in terms of DP compliance, meeting SLOs, and recovering data in the event of data loss

**Leaders**
- 12%
- Place a very high value on data (data = capital)
- Have DP solutions that will meet all or most future challenges
- Advanced use of public cloud for DP
- Recovery times under 2 hours
- Highly confident in terms of DP compliance, meeting SLOs, and recovering data in the event of data loss
## Maturity rank by country

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>Percentage of Leaders in 2018</th>
<th>Difference (vs. 2016 ranking)</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>India</td>
<td>30%</td>
<td>Up 8</td>
</tr>
<tr>
<td>#2</td>
<td>Mainland China</td>
<td>27%</td>
<td>Down 1</td>
</tr>
<tr>
<td>#3</td>
<td>Brazil</td>
<td>23%</td>
<td>Down 2</td>
</tr>
<tr>
<td>#4</td>
<td>Italy</td>
<td>20%</td>
<td>Up 11</td>
</tr>
<tr>
<td>#5</td>
<td>Japan</td>
<td>18%</td>
<td>Up 10</td>
</tr>
<tr>
<td>#6</td>
<td>US</td>
<td>16%</td>
<td>Up 3</td>
</tr>
<tr>
<td>#7</td>
<td>Mexico</td>
<td>15%</td>
<td>Down 1</td>
</tr>
<tr>
<td>#8</td>
<td>Netherlands</td>
<td>13%</td>
<td>Up 7</td>
</tr>
<tr>
<td>#9</td>
<td>South Africa</td>
<td>12%</td>
<td>(-)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>Percentage of Leaders in 2018</th>
<th>Difference (vs. 2016 ranking)</th>
</tr>
</thead>
<tbody>
<tr>
<td>#10</td>
<td>Switzerland</td>
<td>12%</td>
<td>(-)</td>
</tr>
<tr>
<td>#11</td>
<td>Canada</td>
<td>10%</td>
<td>Down 2</td>
</tr>
<tr>
<td>#12</td>
<td>UK</td>
<td>9%</td>
<td>Down 6</td>
</tr>
<tr>
<td>#13</td>
<td>Singapore</td>
<td>9%</td>
<td>Down 11</td>
</tr>
<tr>
<td>#14</td>
<td>UAE</td>
<td>8%</td>
<td>Up 1</td>
</tr>
<tr>
<td>#15</td>
<td>Germany</td>
<td>7%</td>
<td>Down 10</td>
</tr>
<tr>
<td>#16</td>
<td>Australia</td>
<td>5%</td>
<td>Down 10</td>
</tr>
<tr>
<td>#17</td>
<td>France</td>
<td>3%</td>
<td>Down 16</td>
</tr>
<tr>
<td>#18</td>
<td>South Korea</td>
<td>1%</td>
<td>Down 9</td>
</tr>
</tbody>
</table>
FOCUS OF KEY FINDINGS:

1: The value of data
2: Data protection solutions currently in place
3: Challenges surrounding data protection
4: Public cloud – changing the data protection landscape
5: Disruption experience
THE VALUE OF DATA
The ever-increasing volume of data

MANAGE ON AVERAGE

9.70PB

OF DATA IN 2018

IN 2016 IT WAS 1.45PB

(A GROWTH OF 569%)
The value of data

92% SEE THE POTENTIAL VALUE OF DATA

36% CONSIDER DATA TO BE EXTREMELY VALUABLE

- Data is extremely valuable: 36%
- We are investing in tools to help us monetize data in the future: 1%
- We see the potential value that data has: 17%
- Data holds minimal long-term value: 6%
- We have not considered the value of data: 1%
- Don’t know: 1%
The most valuable sources of data

PRODUCTIVITY APPS AND AI/ML CONSIDERED TWO OF THE MOST VALUABLE SOURCES OF DATA

- Productivity (e.g. Office 365) 24%
- Artificial intelligence (AI)/Machine learning (ML) 24%
- BI/analytics systems 23%
- Unstructured data (e.g. video, images, sensor data) 22%
- Data warehouse 22%
- Customer support systems 21%
- Internet of Things (IoT) 21%
- Online internet presence (websites) 20%
- CRM 18%
- Content management systems 16%
- Online social engagement (social networks) 15%
- ERP 14%

Global Data Protection Index 2018 research - Key Findings - Commissioned by Dell EMC
Treating data protection differently for different data sources

81% TAKE DATA PROTECTION MORE SERIOUSLY FOR ‘MORE VALUABLE’ DATA

- We take data protection much more seriously for the data that has the greatest monetary value
- We take data protection slightly more seriously for the data that has the greatest monetary value
- We treat all protection of data equally, regardless of the value of the data

Global Data Protection Index 2018 research - Key Findings - Commissioned by Dell EMC
DATA PROTECTION SOLUTIONS CURRENTLY IN PLACE
76% USE AT LEAST TWO DATA PROTECTION VENDORS
IN MOST CASES, ORGANIZATIONS ARE USING A NUMBER OF DIFFERENT SOLUTIONS – AND LIKELY DIFFERENT VENDORS – SIMULTANEOUSLY.

Data protection solutions used

- Backup: 15.39%
- Replication: 16.48%
- Archive: 17.62%
- Snapshots: 24.52%
- Continuous availability: 25.99%
Backup preferences for long-term retention

PRIVATE CLOUD IS NOW THE MOST POPULAR FOR LONG-TERM RETENTION BUT 30% ARE STILL USING TAPE

<table>
<thead>
<tr>
<th>Backup Method</th>
<th>2018</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backups sent to on premises (or private) cloud</td>
<td>36.15%</td>
<td>36.14%</td>
</tr>
<tr>
<td>Backups sent to public cloud for long term</td>
<td>33.07%</td>
<td>30.06%</td>
</tr>
<tr>
<td>Backups sent to tape for long term</td>
<td>30.06%</td>
<td>30.06%</td>
</tr>
</tbody>
</table>
## Technology currently used in availability strategies

### AUTOMATIC BACKUP TO CLOUD IS THE TECHNOLOGY MOST FREQUENTLY INCLUDED AS PART OF AVAILABILITY STRATEGIES FOR MISSION-CRITICAL WORKLOADS

<table>
<thead>
<tr>
<th>Technology</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic backup to the cloud</td>
<td>43%</td>
</tr>
<tr>
<td>Integrated data protection appliances</td>
<td>33%</td>
</tr>
<tr>
<td>Replication of both applications and data (such as virtual machine images)</td>
<td>32%</td>
</tr>
<tr>
<td>Replication to a second site (including cloud) with restart capabilities (active/passive)</td>
<td>32%</td>
</tr>
<tr>
<td>Disk-based backup and recovery including clones/snaps</td>
<td>31%</td>
</tr>
<tr>
<td>Tape backup and tapes are kept off site (on own premises)</td>
<td>30%</td>
</tr>
<tr>
<td>WAN-based replication of backup and recovery images to second site</td>
<td>26%</td>
</tr>
<tr>
<td>Backup appliance with deduplication</td>
<td>26%</td>
</tr>
<tr>
<td>Dynamic mobility of virtual applications between data centers</td>
<td>26%</td>
</tr>
<tr>
<td>Disaster tolerant replication (active/active) with near zero RPO and RTO</td>
<td>26%</td>
</tr>
<tr>
<td>Tape backup and tapes are kept off site (on 3rd party premises)</td>
<td>23%</td>
</tr>
<tr>
<td>Tape backup and tapes go home with employees</td>
<td>16%</td>
</tr>
</tbody>
</table>
Consumption of data protection

CONSUMPTION OF DATA PROTECTION IS CHANGING

SUBSCRIPTION MODELS ARE NOW THE MOST POPULAR METHOD OF CONSUMPTION - MORE POPULAR THAN CAPEX AND OPEX

<table>
<thead>
<tr>
<th>Consumption Method</th>
<th>Total 2016</th>
<th>Total 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription (you subscribe to a set amount of devices or capacity upfront)</td>
<td>21%</td>
<td>6%</td>
</tr>
<tr>
<td>Capital purchases (CapEx)</td>
<td>45%</td>
<td>46%</td>
</tr>
<tr>
<td>Operational lease (OpEx)</td>
<td>46%</td>
<td>44%</td>
</tr>
<tr>
<td>Utility pricing/ad hoc pay as you go</td>
<td>49%</td>
<td>40%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>6%</td>
<td>3%</td>
</tr>
</tbody>
</table>

Global Data Protection Index 2018 research - Key Findings - Commissioned by Dell EMC
CHALLENGES SURROUNDING DATA PROTECTION
Data protection challenges

95% of respondents’ organizations are facing at least one challenge in relation to data protection.

- Complexity of configuring and operating data protection software and/or hardware: 46%
- Ballooning costs of storing and managing backup copies because of rapid data growth: 46%
- Lack of data protection solutions for newer technologies: 45%
- Ensuring that we stay compliant with regulations (e.g. GDPR) that relate to this: 41%
- Inability to keep track of and protect all data because of growth of DevOps and cloud development teams: 40%
- Inability to meet backup windows because of hardware performance or network bottlenecks: 35%
- Inability to meet backup windows because of growth in size of databases: 31%
Lack of data protection solutions for newer technology

FOR THOSE WHO ARE STRUGGLING TO FIND SOLUTIONS FOR NEWER TECHNOLOGIES...

51% CANNOT FIND SUITABLE DATA PROTECTION SOLUTIONS FOR AI/ML

WE CAN’T FIND DATA PROTECTION SOLUTIONS FOR...

- Artificial intelligence/machine learning: 51%
- Cloud-native applications: 47%
- IoT: 40%
- Robotic process automation: 33%
- Chatbots/virtual assistants: 30%
- Containers: 28%
Confidence in current data protection solutions

ONLY

37% ARE VERY CONFIDENT THAT THEIR ORGANIZATION IS MEETING ITS BACKUP AND RECOVERY SLOS

AND ONLY

35% ARE VERY CONFIDENT THAT THEIR DATA PROTECTION INFRASTRUCTURE IS COMPLIANT WITH REGULATIONS
Meeting future business challenges

**ONLY 16%**

BELIEVE THAT THEIR CURRENT DATA PROTECTION SOLUTIONS WILL BE ABLE TO MEET **ALL** FUTURE BUSINESS CHALLENGES

---

**OUR CURRENT DATA PROTECTION SOLUTIONS WILL BE ABLE TO MEET...**

- 7% No future business challenges
- 31% A minority of future business challenges
- 46% The majority of future business challenges
- 16% All future business challenges
PUBLIC CLOUD – CHANGING THE DATA PROTECTION LANDSCAPE
The IT environment in 2018

PUBLIC CLOUD USE HAS INCREASED FROM 28% IN 2016 TO 40% IN 2018

ON-PREMISES SOLUTIONS HAVE SHRUNK FROM 56% IN 2016 TO 38%
98% of those whose organization uses public cloud report that it features as part of their data protection infrastructure.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup/snapshot services to protect workloads developed in public cloud using new application architectures</td>
<td>41%</td>
</tr>
<tr>
<td>Backup of our on-premises workloads and data</td>
<td>41%</td>
</tr>
<tr>
<td>Protecting specific SaaS apps (e.g. Office 365)</td>
<td>40%</td>
</tr>
<tr>
<td>Cloud-enabled versions of our on-premises data protection software to protect our public cloud workloads</td>
<td>40%</td>
</tr>
<tr>
<td>Backup/snapshot services to protect workloads developed in public cloud using legacy application architectures</td>
<td>38%</td>
</tr>
<tr>
<td>Protecting our database management applications which run on public cloud (e.g. MySQL)</td>
<td>36%</td>
</tr>
<tr>
<td>Long term retention</td>
<td>34%</td>
</tr>
<tr>
<td>Disaster recovery</td>
<td>34%</td>
</tr>
<tr>
<td>Archiving</td>
<td>33%</td>
</tr>
<tr>
<td>Mobile device backup</td>
<td>30%</td>
</tr>
<tr>
<td>We do not use public cloud for any part of our data protection</td>
<td>2%</td>
</tr>
</tbody>
</table>
Data protection considerations in the public cloud

Requirements vary by organization when looking at data protection solutions in a public cloud environment.

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>The impact of the data protection infrastructure or services required to protect at scale</td>
<td>41%</td>
</tr>
<tr>
<td>The ability to scale services as public cloud workload increases</td>
<td>40%</td>
</tr>
<tr>
<td>Total cost of ownership (TCO) and hard cost savings for using public cloud for disaster recovery</td>
<td>40%</td>
</tr>
<tr>
<td>Public cloud protection service offerings compared to 3rd party data protection offerings (feature and workload support)</td>
<td>39%</td>
</tr>
<tr>
<td>Visibility of protected cloud infrastructure across multi-regions of the cloud provider</td>
<td>37%</td>
</tr>
<tr>
<td>The possibility to build our own solutions to address public cloud data protection</td>
<td>34%</td>
</tr>
<tr>
<td>Portability or replication of workload between on-prem and multi cloud providers</td>
<td>33%</td>
</tr>
<tr>
<td>Whether we have unified management of backup data stored on-prem and across multi public cloud providers</td>
<td>33%</td>
</tr>
<tr>
<td>The lowest cost public cloud provider or service available</td>
<td>27%</td>
</tr>
<tr>
<td>We do not take data protection into account when using public cloud</td>
<td>2%</td>
</tr>
</tbody>
</table>

Key Findings - Commissioned by Dell EMC
Responsibility for public cloud-based applications

THE IT DEPARTMENT AS A WHOLE IS MOST LIKELY TO BE RESPONSIBLE FOR DATA PROTECTION OF PUBLIC CLOUD-BASED APPLICATIONS

- My IT department as a whole: 43%
- The head of our IT department: 40%
- The IT backup team (they cover both on-premises and public cloud applications): 35%
- The cloud service provider: 32%
- The cloud architect or cloud IT operations team: 32%
- The application/database owner (e.g. Microsoft, SAP, Oracle, etc.): 25%
- Each department in my organization, dependent on their use of the application in question: 23%
DISRUPTION EXPERIENCE
Disruption experiences in the last 12 months

76% of respondents’ organizations have experienced disruption of some kind in the last 12 months

- Unplanned systems downtime: 41%
- Ransomware attack that prevented access to data: 28%
- Data loss: 28%
- Inability to recover data from the current data protection method or product: 27%
- Local disaster which affected access to data for an entire site or group: 25%
- We have not experienced any: 24%
The impact of multiple vendors on disruption

Organizations with a single data protection vendor are less likely to have experienced disruption in the last 12 months.

Unplanned systems downtime: 34% (One vendor) vs. 17% (Two or more vendors)
Ransomware attack that prevented access to data: 32% (One vendor) vs. 21% (Two or more vendors)
Data loss: 29% (One vendor) vs. 21% (Two or more vendors)
Inability to recover data from the current data protection method or product: 29% (One vendor) vs. 21% (Two or more vendors)
Local disaster which affected access to data for an entire site or group: 27% (One vendor) vs. 16% (Two or more vendors)
We have not experienced any: 40% (One vendor) vs. 19% (Two or more vendors)
The cost of unplanned systems downtime

20 HOURS OF DOWNTIME = $526,845
COST IN THE LAST 12 MONTHS, ON AVERAGE

20 hours on average

Less than 1 hour: $84,615
1 - 12 hours: $293,485
12 - 24 hours: $500,213
1 - 2 days: $654,990
2 - 5 days: $1,182,429

Global Data Protection Index 2018 research - Key Findings - Commissioned by Dell EMC
The cost of data loss

2.13TB OF DATA LOST = $995,613 COST IN THE LAST 12 MONTHS, ON AVERAGE

2.13TB on average

Less than 50GB: 6%
50GB - 250GB: 25%
250GB - 500GB: 19%
500GB - 750GB: 18%
750GB - 1TB: 12%
1TB - 5TB: 13%
More than 5TB: 5%
Don't know: 2%
The more you value data, the more it costs to lose it

Not only does the amount of data you lose increase the cost, so does the value of the data itself.

<table>
<thead>
<tr>
<th>Amount</th>
<th>Value Range</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 50GB</td>
<td>$302,529</td>
<td></td>
</tr>
<tr>
<td>50GB - 250GB</td>
<td>$322,921</td>
<td></td>
</tr>
<tr>
<td>250GB - 500GB</td>
<td>$472,740</td>
<td></td>
</tr>
<tr>
<td>500GB - 750GB</td>
<td>$849,988</td>
<td></td>
</tr>
<tr>
<td>750GB - 1TB</td>
<td>$983,519</td>
<td></td>
</tr>
<tr>
<td>1TB - 5TB</td>
<td>$2,406,742</td>
<td></td>
</tr>
<tr>
<td>5TB - 50TB</td>
<td>$3,627,148</td>
<td></td>
</tr>
</tbody>
</table>

We have not considered the value of data.
Data holds minimal long-term value.
We see the potential value that data has.
We are investing in tools to help us monetize data in the future.
Data is extremely valuable.
Recovering from unexpected critical application downtime

ONLY 8% OF RESPONDENTS EXPECT THEIR ORGANIZATION’S RECOVERY TIME TO BE LESS THAN AN HOUR

THE AVERAGE IS 7 HOURS
What are the causes of this disruption?

THERE ARE MANY DIFFERENT CAUSES FOR THIS DISRUPTION, MAKING IT DIFFICULT FOR ORGANIZATIONS TO DEFEND AGAINST

- Hardware failure: 36%
- Software failure: 35%
- Data corruption: 30%
- External security breach (e.g. malware, ransomware): 28%
- Loss of power: 27%
- Accidental user error: 23%
- Loss of backup power: 22%
- The fault of service/cloud providers: 21%
- Internal security breach: 19%
- Physical security (e.g. loss/theft of equipment): 18%
- Natural disaster (e.g. tsunami, hurricane): 16%
- Deliberate employee sabotage: 13%
- The cause is still unknown: 1%
Consequences of data loss and/or systems downtime

96% of organizations that have suffered data loss and/or unplanned systems downtime have experienced consequences.

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of employee productivity</td>
<td>37%</td>
</tr>
<tr>
<td>Inability to provide essential services</td>
<td>30%</td>
</tr>
<tr>
<td>Delay in product/service development</td>
<td>30%</td>
</tr>
<tr>
<td>Loss of revenue</td>
<td>30%</td>
</tr>
<tr>
<td>Delay in getting products/services to market</td>
<td>25%</td>
</tr>
<tr>
<td>Loss of customer confidence/loyalty</td>
<td>24%</td>
</tr>
<tr>
<td>Loss of an incremental business opportunity</td>
<td>19%</td>
</tr>
<tr>
<td>Loss of a new business opportunity</td>
<td>19%</td>
</tr>
<tr>
<td>Loss of customers</td>
<td>19%</td>
</tr>
<tr>
<td>Loss of business to a competitor</td>
<td>18%</td>
</tr>
<tr>
<td>Loss of repeat business</td>
<td>17%</td>
</tr>
<tr>
<td>Punitive fines</td>
<td>12%</td>
</tr>
<tr>
<td>There have been no consequences</td>
<td>4%</td>
</tr>
</tbody>
</table>

Global Data Protection Index 2018 research - Key Findings - Commissioned by Dell EMC
Confidence in current data protection solutions

IN THE EVENT OF A DATA LOSS INCIDENT, ONLY

33% ARE VERY CONFIDENT THAT THEIR ORGANIZATION COULD FULLY RECOVER IN ORDER TO MEET BUSINESS SLOs

IN THE EVENT OF A DESTRUCTIVE CYBERATTACK, ONLY

35% ARE VERY CONFIDENT THAT THEIR ORGANIZATION COULD RELIABLY RECOVER ALL BUSINESS-CRITICAL DATA
Overall confidence when it comes to data protection

Only 8% are very confident that their organization can do all of these...

- meet its backup and recovery SLOs
- have data protection infrastructure and processes that are compliant with regional governance regulations
- fully recover all systems/data (both on-premises and off) to meet business SLOs in the event of a data loss incident
- reliably recover all business-critical data and protect the most critical data in the event of a destructive cyberattack
Conclusions

- Organizations are now managing a greater volume of data than they ever have before and are assigning a greater *value* to that data

- Yet many are still facing disruption, including unplanned systems downtime and data loss – and this is coming at an enormous cost
  - The risk is even greater for Data Protection Leaders as they are the ones assigning the greatest value to data

- In most cases, organizations need to improve their data protection infrastructure – the majority of respondents highlight at least one area that could be improved or that they do not have confidence in
  - This isn’t easy though, with multiple vendors often being used and a complex environment being faced

- Organizations need to be investing in *future-ready* data protection. This includes moving data protection to a cloud environment and ensuring that data protection for emerging technologies (e.g. AI/ML) is also accounted for
APPENDIX – MATURITY MODEL
Question weighting for DPI maturity model

- Q4 – How confident are you that your organization is meeting its backup and recovery service level objectives (SLOs)? 11%
- Q13 - How confident are you that your organization’s existing data protection solutions are able to meet future business challenges? 11%
- Q20 – What value does your organization place on data? 11%
- Q25 – How confident are you that your organization’s current data protection infrastructure and processes are compliant with regional data governance regulations (e.g. GDPR etc.)? 11%
- Q27 – Which of the following does your organization take into consideration when thinking of your organization’s data protection in a public cloud environment? 24%
- Q29 - During an unexpected event causing downtime to your most critical applications, how long is your recovery time? 11%
- Q30 - How confident are you that, in the event of a data loss incident, you can fully recover systems/data today from all platforms, on premises and off premises, in order to meet business service level objectives? 11%
- Q31 - How confident are you that, in the event of a destructive cyberattack (e.g. a ransomware attack), you can reliably recover all business-critical data, ensuring that the most critical business data is protected from the attack? 11%

Methodology: Index based on the performance of respondents’ organizations in terms of their data protection infrastructure and their confidence in it, the value that they place on data, and recovery times during system downtime.

All related questions from research were filtered through, and 138 points allocated across the curve.
Maturity model questions and scores (i)

Q4 – How confident are you that your organization is meeting its backup and recovery service level objectives (SLOs)?

- Not at all confident (0 points)
- Not very confident (1 point)
- Some doubt (5 points)
- Moderately confident (10 points)
- Very confident (15 points)

Maximum score = 15 points

Q13 – How confident are you that your organization’s existing data protection solutions are able to meet future business challenges?

- Our current data protection solutions will not be able to meet any future business challenges (0 points)
- Our current data protection solutions will be able to meet a minority of future business challenges (5 points)
- Our current data protection solutions will be able to meet the majority of future business challenges (10 points)
- Our current data protection solutions will be able to meet all future business challenges (15 points)

Maximum score = 15 points

Q20 – What value does your organization place on data?

- Data is extremely valuable – we are currently monetizing it (i.e. data = capital) (15 points)
- We are investing in data retention and analytics tools that will help us to monetize all relevant data in the future (10 points)
- We see the potential value that data has (5 points)
- Data is just a by-product of our business process and holds minimal long-term value (0 points)
- We have not considered the value that data may bring to our business (0 points)
- Don’t know (0 points)

Maximum score = 15 points
Q25 – How confident are you that your organization’s current data protection infrastructure and processes are compliant with regional data governance regulations (e.g. GDPR etc.)?

- Not at all confident (0 points)
- Not very confident (1 point)
- Some doubt (5 points)
- Moderately confident (10 points)
- Very confident (15 points)

Maximum score = 15 points

Q27 – Which of the following does your organization take into consideration when thinking of your organization’s data protection in a public cloud environment?

*Please select all that apply*

- The possibility to build our own solutions to address public cloud data protection (3 points)
- The lowest cost public cloud provider or service available (1 point)
- Public cloud protection service offerings compared to 3rd party data protection offerings (feature and workload support) (3 points)
- The ability to scale services as public cloud workload increases (5 points)
- The impact of the data protection infrastructure or services required to protect at scale (5 points)
- Whether we have unified management of backup data stored on-prem and across multi public cloud providers (5 points)
- Visibility of protected cloud infrastructure across multi-regions of the cloud provider (3 points)
- Portability or replication of workload between on-prem and multi cloud providers (3 points)
- Total cost of ownership (TCO) and hard cost savings for using public cloud for disaster recovery (5 points)
- We do not take data protection into account when using public cloud (exclusive) (0 points)

Maximum score = 33 points
Maturity model questions and scores (iii)

Q29 – During an unexpected event causing downtime to your most critical applications, how long is your recovery time?

- Our recovery time is more than one working day (please specify in days) (0 points)
- Our recovery time is 12 - 24 hours (2 points)
- Our recovery time is 6 - 12 hours (4 points)
- Our recovery time is 3 - 6 hours (6 points)
- Our recovery time is 2 - 3 hours (8 points)
- Our recovery time is 1 - 2 hours (10 points)
- Our recovery time is less than an hour (12 points)
- Our recovery time is zero (15 points)
- I do not know (0 points)

Maximum score = 15 points

Q30 – How confident are you that, in the event of a data loss incident, you can fully recover systems/data today from all platforms, on premises and off premises, in order to meet business service level objectives?

- Not at all confident (0 points)
- Not very confident (1 point)
- Some doubt (5 points)
- Moderately confident (10 points)
- Very confident (15 points)

Maximum score = 15 points

Q31 – How confident are you that, in the event of a destructive cyberattack (e.g. a ransomware attack), you can reliably recover all business-critical data, ensuring that the most critical business data is protected from the attack?

- Not at all confident (0 points)
- Not very confident (1 point)
- Some doubt (5 points)
- Moderately confident (10 points)
- Very confident (15 points)

Maximum score = 15 points
ARE YOU PROTECTED?

GET AHEAD OF THE CURVE

DELL EMC – GLOBAL DATA PROTECTION INDEX 2018