Are You Protected

Get Ahead of the Curve
DEMOGRAPHICS

INTERVIEWED
2,200
IT DECISION-MAKERS
IN 3 REGIONS:

INDINDEPENDENT RESEARCH AND ANALYSES: V ANSON BOURNE

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

11 INDUSTRIES
Maturity Curve
MATURITY INDEX

Maturity scored between 1–100 points*

More points awarded for:
- Shorter recovery times
- Confidence in backup infrastructure
- Modern backup systems
- Off-site replication

Points awarded based on the maturity of their data protection strategy

* Exact scoring included in appendix – questions show points used for the original model with a maximum score of 68. All scores multiplied by a factor of 1.47 to create a model of 100 points.
DATA PROTECTION MATURITY CURVE

ONLY ABOUT 1 IN 10 ORGANIZATIONS ARE CONSIDERED TO BE “AHEAD OF THE CURVE” (ADOPTERS AND LEADERS)

- LEADERS (SCORED 76-100 POINTS)
- ADOPTERS (SCORED 51-75 POINTS)
- EVALUATORS (SCORED 26-50 POINTS)
- LAGGARDS (SCORED 1-25 POINTS)
PROFILE CHARACTERISTICS

Laggards
- 38%
  - Archive to tape
  - Back up to tape
  - Recovery time more than 1 day
  - Not confident in ability to restore
  - Backup is core component of strategy

Evaluators
- 52%
  - Archive to disk
  - Back up to disk
  - Recovery time 6 – 24 hours
  - Doubtful of ability to restore
  - Replication is core component of strategy

Adopters
- 9%
  - Use archiving application with offsite replication
  - Back up with de-duplication and offsite replication
  - Recovery time 2-5 hours
  - Moderately confident of ability to restore
  - Active-active instances are core component of strategy

Leaders
- 2%
  - Use archiving application with retention policies
  - Disaster tolerant replication with near-zero RPO/RTO
  - Recovery time 1 hour or less
  - Very confident of ability to restore
  - Standby or virtualized servers are core component of strategy
## MATURITY RANK

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>Businesses ahead of the curve*</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>China</td>
<td>20.0 %</td>
</tr>
<tr>
<td>2</td>
<td>Mexico</td>
<td>17.0 %</td>
</tr>
<tr>
<td>3</td>
<td>Switzerland</td>
<td>16.0 %</td>
</tr>
<tr>
<td>4</td>
<td>Singapore</td>
<td>16.0 %</td>
</tr>
<tr>
<td>5</td>
<td>France</td>
<td>14.5 %</td>
</tr>
<tr>
<td>6</td>
<td>Germany</td>
<td>13.5 %</td>
</tr>
<tr>
<td>7</td>
<td>UK</td>
<td>13.5 %</td>
</tr>
<tr>
<td>8</td>
<td>India</td>
<td>13.0 %</td>
</tr>
<tr>
<td>9</td>
<td>South Africa</td>
<td>11.0 %</td>
</tr>
<tr>
<td>10</td>
<td>Brazil</td>
<td>10.0 %</td>
</tr>
<tr>
<td>11</td>
<td>Italy</td>
<td>9.0 %</td>
</tr>
<tr>
<td>12</td>
<td>South Korea</td>
<td>9.0 %</td>
</tr>
<tr>
<td>13</td>
<td>Australia</td>
<td>8.0 %</td>
</tr>
<tr>
<td>14</td>
<td>USA</td>
<td>8.0 %</td>
</tr>
<tr>
<td>15</td>
<td>Canada</td>
<td>4.0 %</td>
</tr>
<tr>
<td>16</td>
<td>Netherlands</td>
<td>2.0 %</td>
</tr>
<tr>
<td>17</td>
<td>Japan</td>
<td>1.0 %</td>
</tr>
<tr>
<td>18</td>
<td>UAE</td>
<td>0.0 %</td>
</tr>
</tbody>
</table>
Current IT Infrastructure
DATA MANAGEMENT AND PROTECTION

MANAGE ON AVERAGE

1.45PB

OF DATA
57% USE 2 OR MORE DATA PROTECTION VENDORS
56% of organizations’ IT environment is on-premise.

29% is now in the public cloud.
26.99% ... MOST LIKELY TO BE PROTECTING DATA VIA BACKUP
36% BACKUPS ARE SENT TO TAPE RATHER THAN DISK FOR LONG TERM RETENTION
SERVICE LEVEL AGREEMENTS

ONLY 20% REPORT THAT IT HAS BECOME SIGNIFICANTLY EASIER TO ACHIEVE BACKUP AND RECOVERY SLAS

- It is significantly easier than it has been in the past
- It is somewhat easier than it has been in the past
- It is about the same as it has always been
- It is somewhat more difficult than it has been in the past
- It is significantly more difficult than it has been in the past
### DATA PROTECTION CONSUMPTION

**RESPONDENTS ARE MOST LIKELY TO BE CONSUMING DATA PROTECTION THROUGH AN OPERATIONAL LEASE**

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational lease (OpEx)</td>
<td>49%</td>
</tr>
<tr>
<td>Capital purchases (CapEx)</td>
<td>46%</td>
</tr>
<tr>
<td>Utility pricing/ad hoc pay as you go</td>
<td>30%</td>
</tr>
<tr>
<td>Subscription (you subscribe to a set amount of devices or...)</td>
<td>21%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>6%</td>
</tr>
</tbody>
</table>

© Copyright 2016 EMC Corporation. All rights reserved.
Experience of Distribution
CAUSES OF DISRUPTION

UNPLANNED SYSTEMS DOWNTIME

52%

DATA LOSS

29%

LOCAL DISASTER WHICH AFFECTED ACCESS TO DATA FOR AN ENTIRE SITE OR GROUP

23%

INABILITY TO RECOVER DATA FROM THE CURRENT DATA PROTECTION METHOD OR PRODUCT

14%
SUFFERING DATA LOSS OR UNPLANNED SYSTEMS DOWNTIME

HARDWARE FAILURE #1 CAUSE OF DATA LOSS AND/OR SYSTEMS DOWNTIME

- Hardware failure: 45%
- Loss of power: 35%
- Software failure: 34%
- Data corruption: 24%
- External security breach: 23%
- Accidental user error: 20%
- Loss of backup power: 19%
- Internal security breach: 16%
- Physical security: 14%
- Fault of service/cloud providers: 10%
- Deliberate employee sabotage: 10%
- Natural disaster: 08%
- The cause is still unknown: 01%
SUFFERING DATA LOSS OR UNPLANNED SYSTEMS DOWNTIME

36%
REPORTED INTERNAL OR EXTERNAL SECURITY BREACHES

- Hardware failure: 45%
- Loss of power: 35%
- Software failure: 34%
- Data corruption: 24%
- External security breach: 23%
- Accidental user error: 20%
- Loss of backup power: 19%
- Internal security breach: 16%
- Physical security: 14%
- Fault of service/cloud providers: 10%
- Deliberate employee sabotage: 10%
- Natural disaster: 08%
- The cause is still unknown: 01%
AMOUNT OF DATA LOSS IN LAST 12 MONTHS

ON AVERAGE
2.36 TB

DATA LOSS INCREASED WHEN USING MORE VENDORS

<table>
<thead>
<tr>
<th>Solution</th>
<th>Data Loss (TB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>We do not have a data protection solution</td>
<td>4.02</td>
</tr>
<tr>
<td>We built our own solution</td>
<td>2.28</td>
</tr>
<tr>
<td>Data protection solution from one vendor</td>
<td>0.83</td>
</tr>
<tr>
<td>Data protection solution from two vendors</td>
<td>2.04</td>
</tr>
<tr>
<td>Data protection solution from three vendors</td>
<td>2.58</td>
</tr>
<tr>
<td>Data protection solution from four or more vendors</td>
<td>5.47</td>
</tr>
<tr>
<td>Total</td>
<td>2.36</td>
</tr>
</tbody>
</table>
## COST OF DATA LOSS

**OVER $900,000 AVERAGE COST**

**COST TEND TO GO UP WITH MORE VENDORS**

<table>
<thead>
<tr>
<th>Data Protection Solution</th>
<th>Total Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>We do not have a data protection solution</td>
<td>$913,958</td>
</tr>
<tr>
<td>We built our own solution</td>
<td>$517,700</td>
</tr>
<tr>
<td>Data protection solution from one vendor</td>
<td>$973,361</td>
</tr>
<tr>
<td>Data protection solution from two vendors</td>
<td>$636,110</td>
</tr>
<tr>
<td>Data protection solution from three vendors</td>
<td>$789,193</td>
</tr>
<tr>
<td>Data protection solution from four or more vendors</td>
<td>$911,030</td>
</tr>
</tbody>
</table>

* AVERAGE COST
$555,000 is the average cost of unplanned system downtime.
UNPLANNED SYSTEM DOWNTIME

22 HOURS IS THE AVERAGE LENGTH OF DOWNTIME

DOWNTIME INCREASED WITH MORE VENDORS

- Total: 22 hours
- We do not have a data protection solution: 24 hours
- We built our own solution: 19 hours
- Data protection solution from one vendor: 19 hours
- Data protection solution from two vendors: 21 hours
- Data protection solution from three vendors: 23 hours
- Data protection solution from four or more vendors: 37 hours
DATA PROTECTION PREPAREDNESS

ONLY 18% THINK THAT THEIR CURRENT DATA PROTECTION SOLUTIONS WILL MEET ALL FUTURE BUSINESS CHALLENGES

- Our current data protection solutions will not be able to meet any future business challenges
- Our current data protection solutions will be able to meet a minority of future business challenges
- Our current data protection solutions will be able to meet some future business challenges
Recovery Methods
AVAILABILITY

BACKUP IS THE MOST POPULAR AVAILABILITY STRATEGY WITH 41% USING AUTOMATIC BACKUP TO THE CLOUD
RECOVERY TIME FOR CRITICAL APPS

ONLY 9%
CAN RECOVER IN LESS
THAN AN HOUR

ON AVERAGE, IT TAKES
7 HOURS TO RECOVER

- Recovery time is > 1 working day
- Recovery time is 12-24 hours
- Recovery time is 6-12 hours
- Recovery time is 3-6 hours
- Recovery time is 2-3 hours
- Recovery time is 1-2 hours
- Recovery time is < 1 hour
- I do not know

© Copyright 2016 EMC Corporation. All rights reserved.
ARCHIVING

BACKUP TO TAPE FOLLOWED BY DISK IS MOST LIKELY ARCHIVE STRATEGY.

5 YEARS AVERAGE DATA RETENTION REQUIREMENT

- No archiving strategy (14%)
- Data onto tape (27%)
- Data online (e.g. onto disk) (34%)
- Data to appliances (18%)
- Data to appliances w/copy off site (7%)
Business Alignment
PUBLIC CLOUD IS BEING USED FOR A WIDE RANGE OF APPLICATIONS

- Email: 87%
- Online internet presence: 85%
- Productivity: 83%
- Archiving: 81%
- CRM: 80%
- Customer support systems: 80%
- Content management systems: 79%
- Data warehouse: 78%
- Content distribution systems: 77%
- BI/analytics systems: 77%
- ERP: 76%
- Payroll: 73%
VARIED APPROACHES FOR MANAGING DATA PROTECTION IN PUBLIC CLOUDS

LESS THAN $\frac{1}{2}$ SAY ALL DATA STORED IN THE CLOUD IS PROTECTED AGAINST DELETION AND CORRUPTION

<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>The head of our IT department</td>
<td>58%</td>
</tr>
<tr>
<td>The cloud service provider</td>
<td>47%</td>
</tr>
<tr>
<td>My IT department as a whole</td>
<td>45%</td>
</tr>
<tr>
<td>Each department in my organisation, dependent on...</td>
<td>13%</td>
</tr>
<tr>
<td>I do not know</td>
<td>2%</td>
</tr>
</tbody>
</table>
90% of organizations are using public cloud for data protection.

- We use public cloud for archiving: 46%
- We use public cloud for protecting specific apps: 45%
- We use public cloud for long term retention: 43%
- We use public cloud for mobile device backup: 33%
- We use public cloud for disaster recovery: 21%
- We do not use public cloud for any part of our data: 10%
PROTECTION OF FLASH ARRAYS

Only 24% are very confident their data protection solution will keep pace with flash.

9 in 10 (89%) report that they are using, or plan to use, flash arrays.

9 in 10 are using or plan to use flash arrays.
83% SAY DATA PROTECTION IS A MANDATORY OR VERY IMPORTANT CRITERIA WHEN SELECTING A CONVERGED INFRASTRUCTURE SOLUTION

- Yes, it’s a mandatory requirement
- Yes, it’s a very important feature in any decision
- Yes, it’s somewhat important but does not have a strong bearing on any decision
- No, it’s not important
COPY DATA MANAGEMENT

9 IN 10 RESPONDED THAT COPY DATA MANAGEMENT IS VALUABLE

37% REPORT IMPLEMENTING CDM

Yes, we are beginning to see storage growth due to multiple copies

Yes, and we are implementing such solutions

Yes, and we are looking at such solutions

Yes, but do not understand how we can manage the proliferation of copies

No, it would not reduce costs

© Copyright 2016 EMC Corporation. All rights reserved.
Management
WHO MANAGES DATA PROTECTION?

MANAGEMENT AlignS WITH ENVIRONMENT

STORAGE BASED PROTECTION = STORAGE TEAM

NON-STORAGE BASED PROTECTION = BACKUP TEAM

VIRTUAL PROTECTION = VIRTUALIZATION TEAM

<table>
<thead>
<tr>
<th></th>
<th>Storage team</th>
<th>Backup team</th>
<th>Virtualisation team</th>
<th>Each application team manages their own</th>
<th>Don't know</th>
</tr>
</thead>
<tbody>
<tr>
<td>28%</td>
<td>25%</td>
<td>32%</td>
<td>20%</td>
<td>14%</td>
<td>4%</td>
</tr>
<tr>
<td>25%</td>
<td>40%</td>
<td>26%</td>
<td>26%</td>
<td>18%</td>
<td>6%</td>
</tr>
<tr>
<td>40%</td>
<td>45%</td>
<td>40%</td>
<td>40%</td>
<td>17%</td>
<td>6%</td>
</tr>
</tbody>
</table>

© Copyright 2016 EMC Corporation. All rights reserved.
40% PREFER A COLLABORATIVE MODEL

- Collaborative model (infrastructure teams and application owners)
- Single authority group
- They are of equal importance
- Don’t know
Over 84% respondents state that central visibility across all clouds environments is essential.

- 38% Yes, it is absolutely essential
- 47% Yes, it is somewhat essential
- 12% No, not essential as long as there is visibility of protection status
- 4% No, not essential regardless if application owners have visibility of protection status
93% report that data protection solutions that integrate directly into business applications are valuable.
CONCLUSIONS

• Data loss and downtime are expensive with new threats like cyber attacks emerging

• Most companies globally are behind the curve and lacking confidence that their data protection solutions will cover all future requirements

• Data growth continues and the shift to the cloud is rapidly reshaping the IT landscape potentially exposing more data

• Attacking data protection through multiple vendors tends to increase cost and risk

• Modernizing data protection means considering a continuum of technologies to meet all business needs as well evolving data protection for new demands like cloud, flash, CI, CDM
RECOMMENDATIONS

1. Validate you have an appropriate data protection solution in place for all of your critical data no matter where it is or how it is generated. EMC and our partners can help you with a gap analysis assessment process.

2. Modernize your data protection strategy to maintain a level of visibility and control for application owners while exploring how automation for Data Protection can add value to your organization.

3. Evaluate any gaps in your protection strategy that have emerged from disparate vendor solutions being used to meet your changing Data Protection needs.

4. When you look at CI/HCI solitons as part of your digital transformation, validate how your data protection needs will be met or if additional vendor point solutions are still required.

5. Validate your Cloud apps and SaaS solution data protection needs. Remember Cloud solutions (Public Cloud or SaaS solutions) don’t natively include Data Protection with the same level of protection your business is accustomed to receive today.