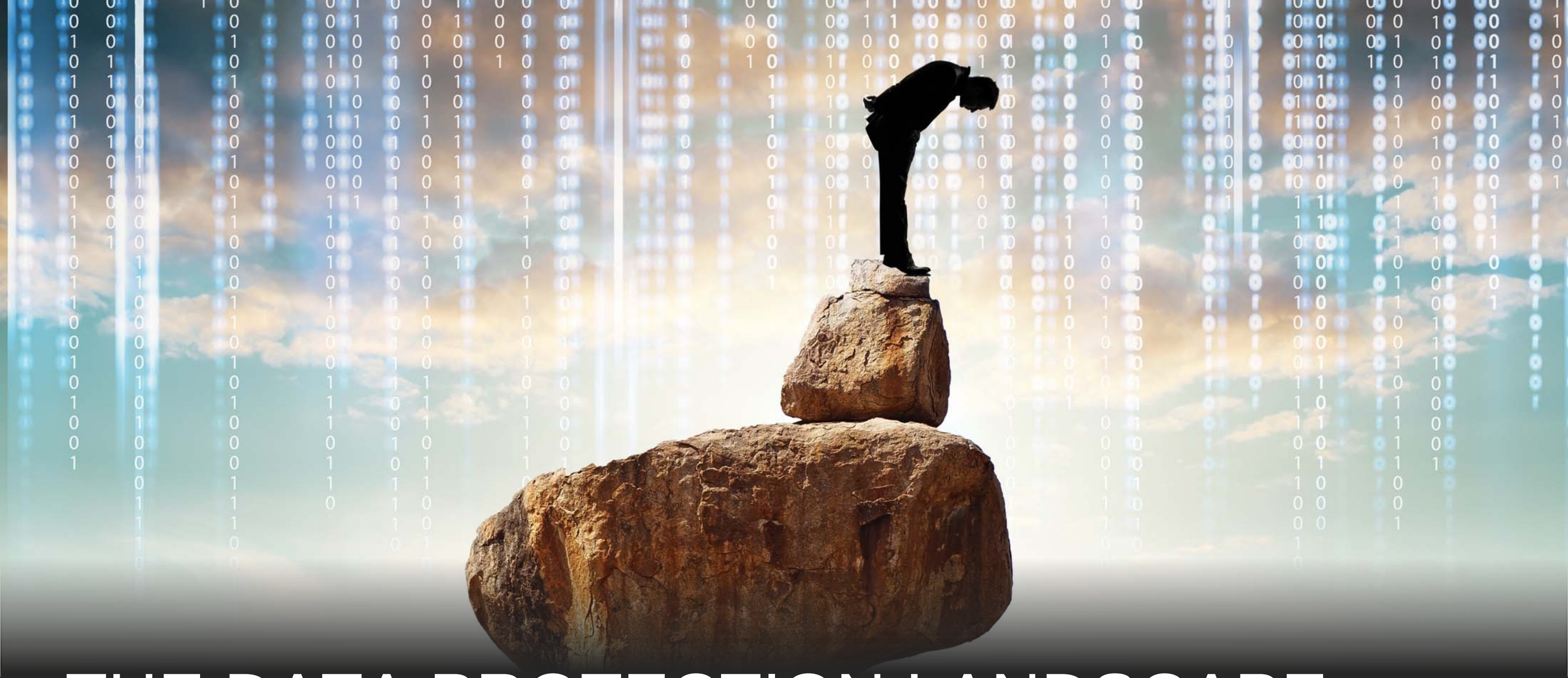
EMC GLOBAL DATA PROTECTION INDEX

KEY FINDINGS & RESULTS FOR **ITALY**



THE DATA PROTECTION LANDSCAPE

ARE YOU ON SOLID GROUND?

EMC²

GLOBAL KEY FINDINGS

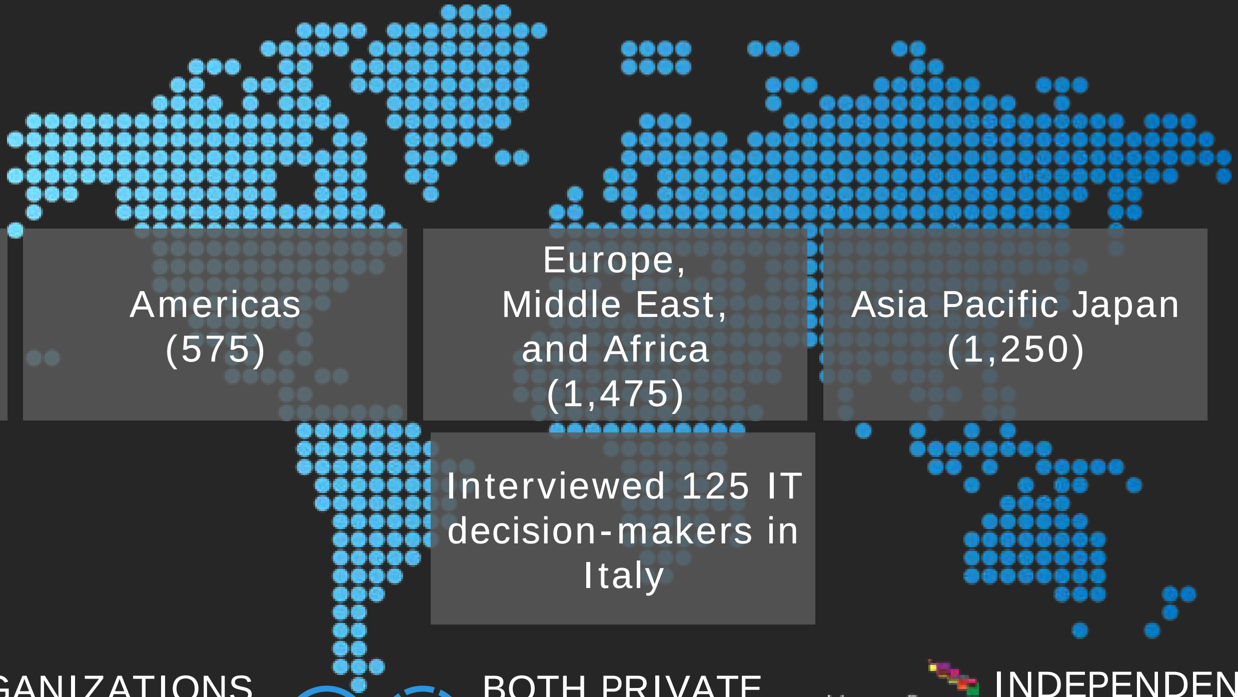
GLOBALLY, ENTERPRISES ARE LOSING AS MUCH AS $1.7 TRILLION THROUGH DATA LOSS AND UNPLANNED DOWNTIME

62% of respondents said at least one of the following: big data, hybrid cloud, mobile devices, is 'difficult' or 'very difficult' to protect

Adopting advanced data protection tools leads to reduced data loss

87% of businesses are behind the curve for data protection maturity and 71% of businesses are not fully confident of restoring their data

DEMOGRAPHICS



INTERVIEWED 3,300 IT DECISION-MAKERS IN 3 REGIONS:

Americas (575)

Europe, Middle East, and Africa (1,475)

Asia Pacific Japan (1,250)

Interviewed 125 IT decision-makers in Italy

24 COUNTRIES TOTAL

ORGANIZATIONS OF 250 OR MORE EMPLOYEES

BOTH PRIVATE AND PUBLIC ORGANIZATIONS

INDEPENDENT RESEARCH AND ANALYSIS

DATA PROTECTION MATURITY

MATURITY INDEX

Points awarded based on the maturity of their data protection strategy

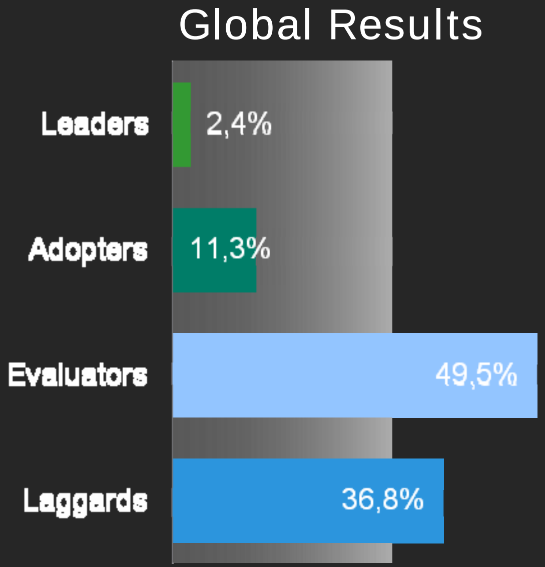
Maturity scored between 1–100 points*

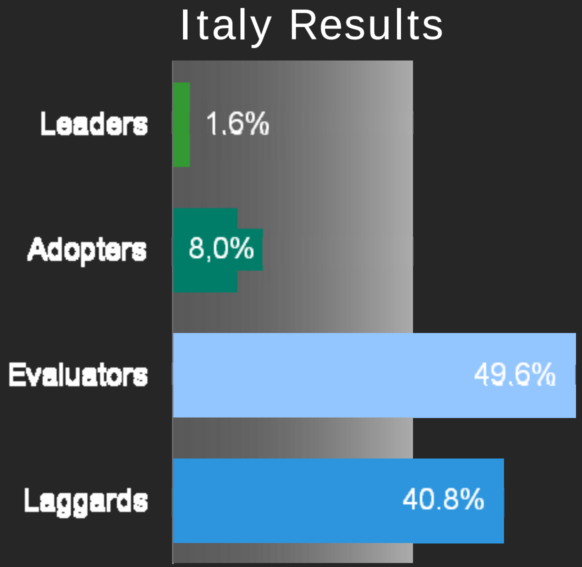
More points awarded for:

- Shorter recovery times
- Confidence in backup infrastructure
- Modern backup systems
- Off-site replication

* 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

WHO IS LEADING THE WAY?





- Leaders (scored 76-100 points)
- Adopters (scored 51-75 points)

AHEAD OF 'MATURITY' CURVE

- Evaluators (scored 26-50 points)
- Laggards (scored 1-25 points)

Figure 1: Analysis of maturity
Base: all respondents (3,300)

Figure 2: Analysis of maturity
Base: all respondents from Italy (125)

GLOBAL IT MATURITY

SHOWING FREQUENCY OF POINTS SCORED

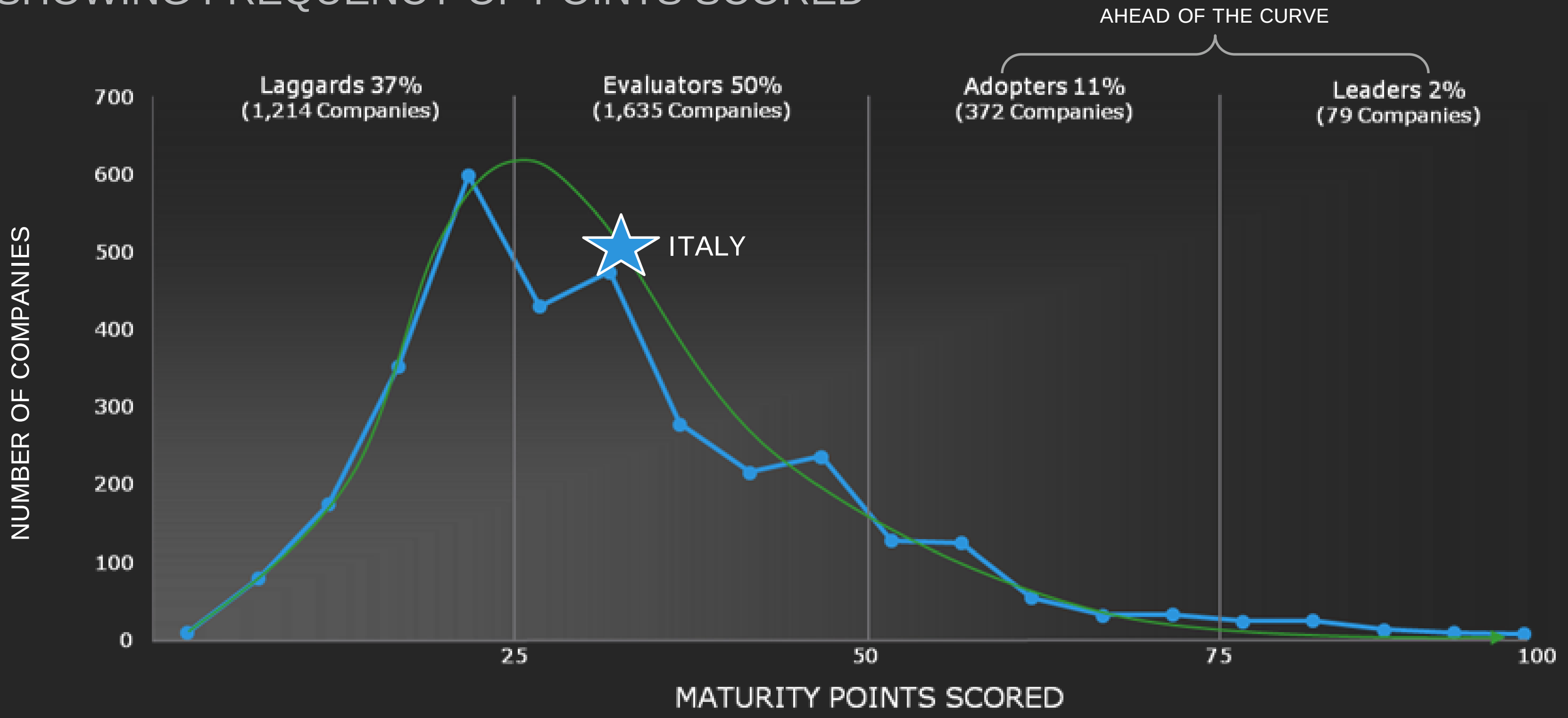
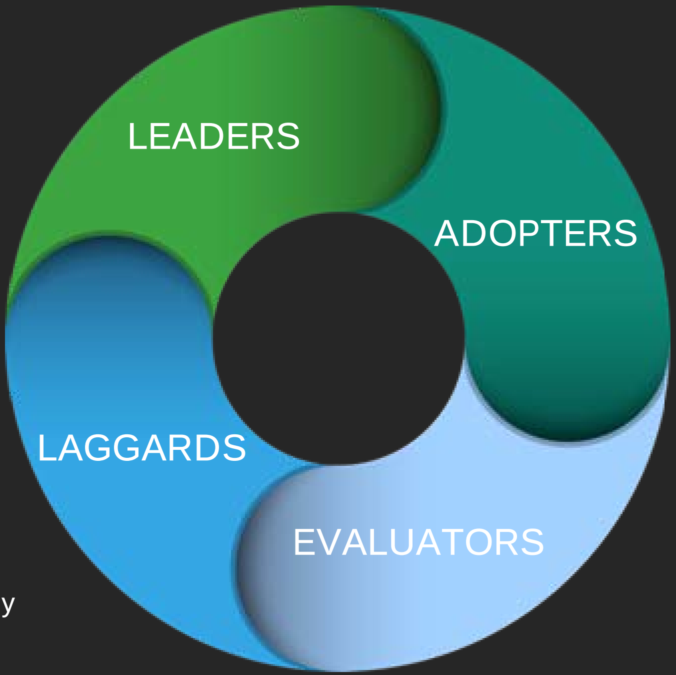


Figure 3: Analysis of maturity – showing frequency of points scored
Base: all respondents (3300)

PROFILE CHARACTERISTICS

- 🟦 Use archiving application with retention policies
- 🟩 Disaster tolerant replication with near-zero RPO/RTO
- 🟨 Recovery time one hour or less
- 🟧 Very confident of ability to restore
- 🟥 Standby or virtualized servers are core component of strategy

- 🟦 Use archiving application with offsite replication
- 🟩 Backup with deduplication & offsite replication
- 🟨 Recovery time 2 – 5 hours
- 🟧 Moderately confident of ability to restore
- 🟥 Active-active instances are core component of strategy



- 🟦 Archive to tape
- 🟩 Backup to tape
- 🟨 Recovery time more than one day
- 🟧 Not confident in ability to restore
- 🟥 Backup is core component of strategy

- 🟦 Archive to disk
- 🟩 Backup to disk
- 🟨 Recovery time 6 – 24 hours
- 🟧 Doubtful of ability to restore
- 🟥 Replication is core component of strategy

WHERE ARE THE MOST MATURE ORGANISATIONS?

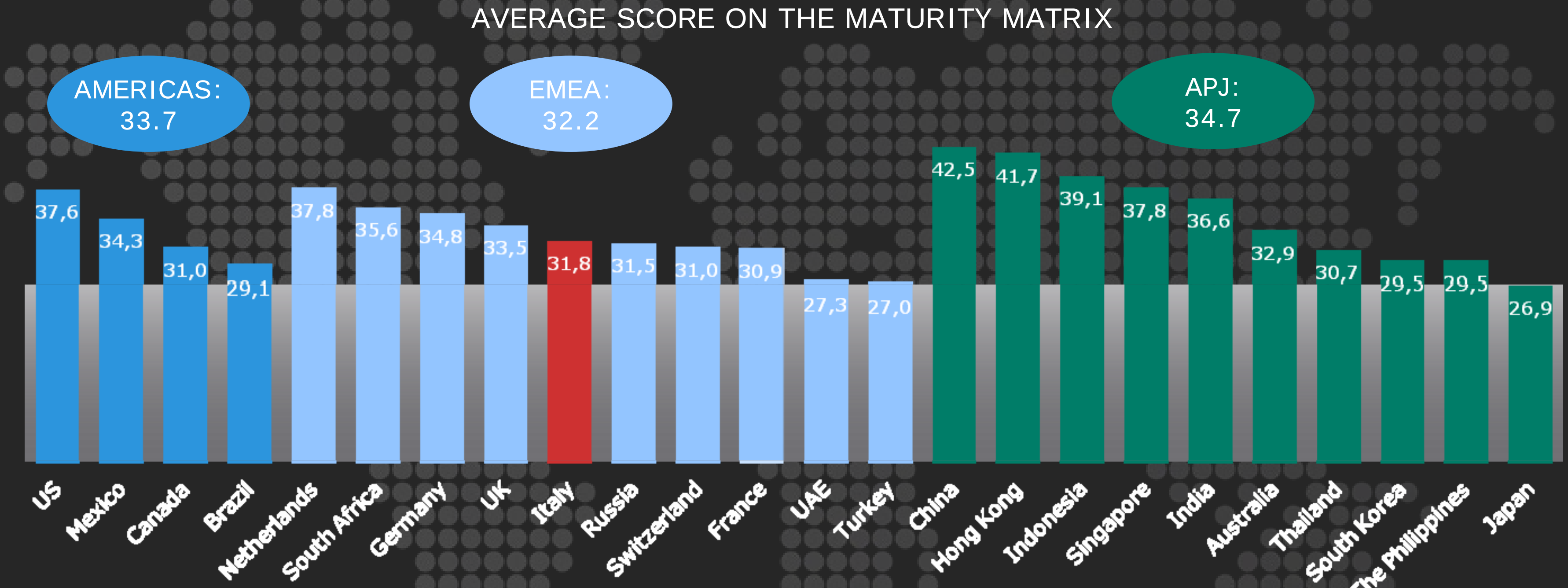


Figure 4: Analysis of average maturity score by region and country
Base: all respondents (3300)

MATURITY RANK

WHICH MARKETS ARE AHEAD?

- Businesses in **China** and **Hong Kong** most likely to be ahead of the curve
- Outside of Asia, the **US** and the **Netherlands** most likely to be ahead of the curve
- **UAE, Turkey** and **Switzerland** and least likely to be ahead of maturity curve

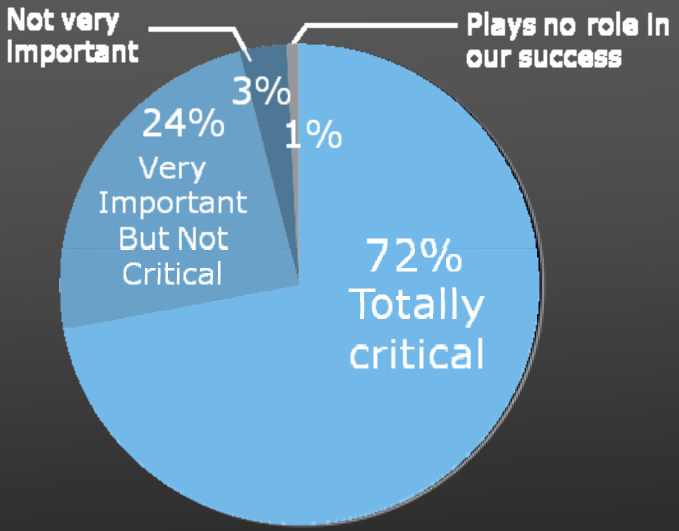
RANK	COUNTRY	% OF BUSINESSES AHEAD OF MATURITY CURVE*
1	China	29.6%
2	Hong Kong	27.2%
3	Netherlands	20.8%
4	Singapore	20.0%
5	USA	19.5%
6	India	19.2%
7	South Africa	18.4%
8	Indonesia	18.4%
9	Mexico	17.6%
10	Germany	15.5%
11	Australia	14.4%
12	UK	13.0%
13	The Philippines	11.2%
14	Thailand	11.2%
15	Canada	9.6%
16	Russia	9.6%
17	Italy	9.6%
18	Brazil	8.8%
19	Japan	8.0%
20	South Korea	8.0%
21	France	6.5%
22	Switzerland	6.4%
23	Turkey	5.6%
24	UAE	0.0%

*Please note that the percentages have been rounded to one decimal place

THE IMPORTANCE OF DATA PROTECTION

THE CRITICALITY OF DATA PROTECTION

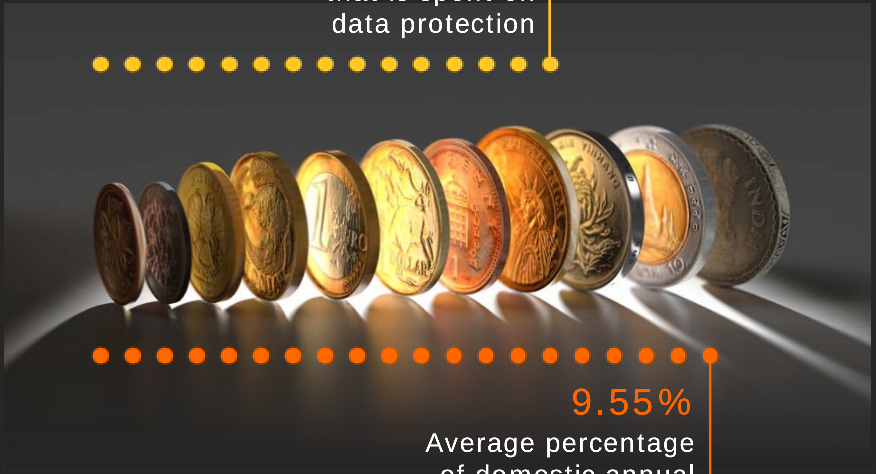
DO YOU CONSIDER DATA PROTECTION CRITICAL TO THE SUCCESS OF YOUR organization?



- Around three quarters (72%) of respondents consider data protection to be totally critical to their organization’s success
- The financial services sector (83%) and public sector (82%) are most likely to see data protection as totally critical, compared with 64% from the IT sector

Figure 5: “Do you consider data protection to be totally critical to the ongoing success of your organization?”
Base: all respondents (125)

SPENDING ON DATA PROTECTION



8.42%
Average percentage of annual IT budget that is spent on data protection

9.55%
Average percentage of domestic annual revenue that is spent annually on IT

Figure 6: Analysis of average spend of revenue on IT, and of IT budget on data protection
Base: all respondents (125)

Average company spend:

- $211 million on IT
- $14 million on data protection

- The public sector (10.17%) spend the most on data protection

- Organizations under 1,000 employees spend around 7% on data protection

THE NUMBER OF DATA PROTECTION VENDORS

27% Have one vendor

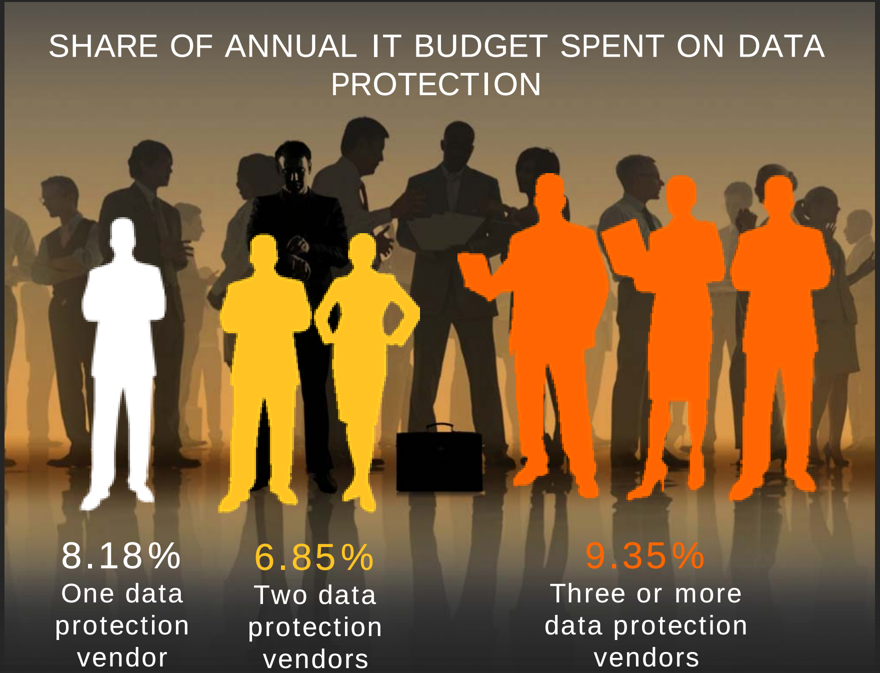
6% Have no specific vendor

67% Have more than one vendor

- 67% have more than one data protection vendor
  - Three vendors on average
- Over eight in ten from the manufacturing (87%) and the financial services (83%) sectors have multiple vendors, compared to 55% from the public sector

Figure 7: “Is your data protection infrastructure built on technology from more than one vendor?”
Base: all respondents (125)

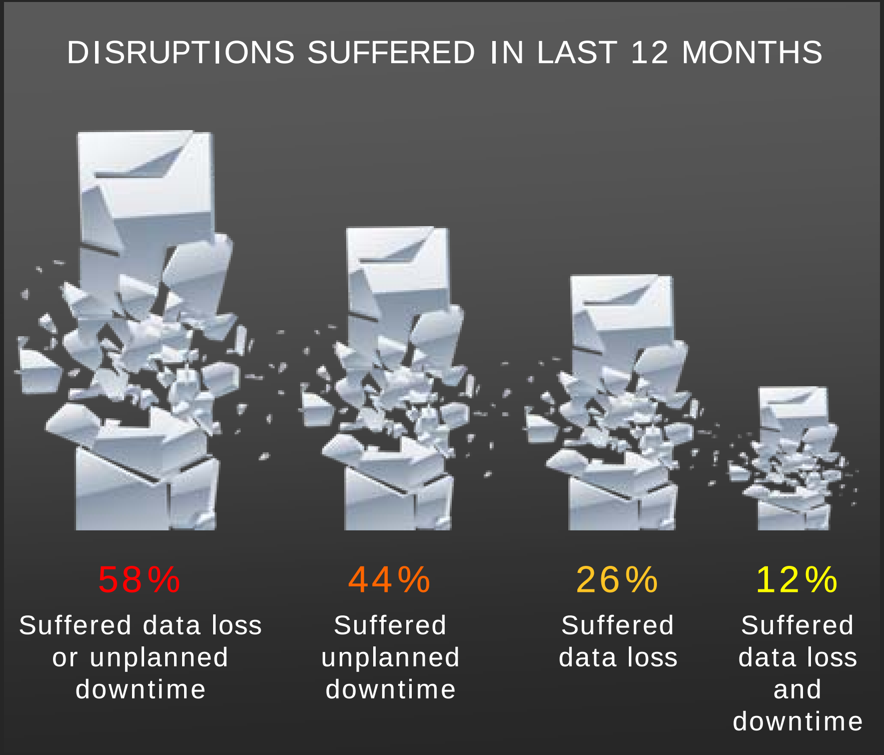
THE EFFECT OF NUMBER OF VENDORS ON SPEND



- The more vendors a business has, the greater proportional spend of IT budget on data protection
- In Italy, those with three vendors are spending 9.35% compared to 8.18% with one vendor

Figure 8: Analysis of average spend of IT budget on data protection, cut by number of data protection vendors
Base: all respondents (125)

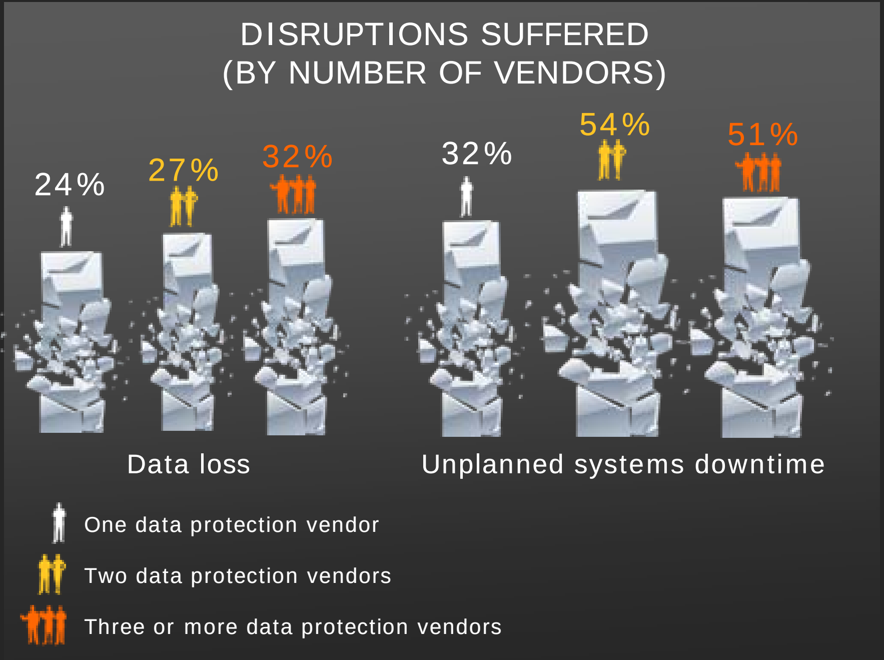
SUFFERING DISRUPTIONS



- 58% have suffered disruptions in the last 12 months
  - 68% public sector
  - 58% IT and telecoms
  - 50% of financial Services
- 68% of organizations with 500-999 employees suffered disruptions
- Average annual loss per company
  - 3.20TB of data (compared to 302GB on average in 2011)
  - Equivalent to around 32 million e-mails
  - Costs $1.17 million

Figure 9: “Has your organization suffered from either unplanned systems downtime or data loss in the last 12 months?”
Base: all respondents (125)

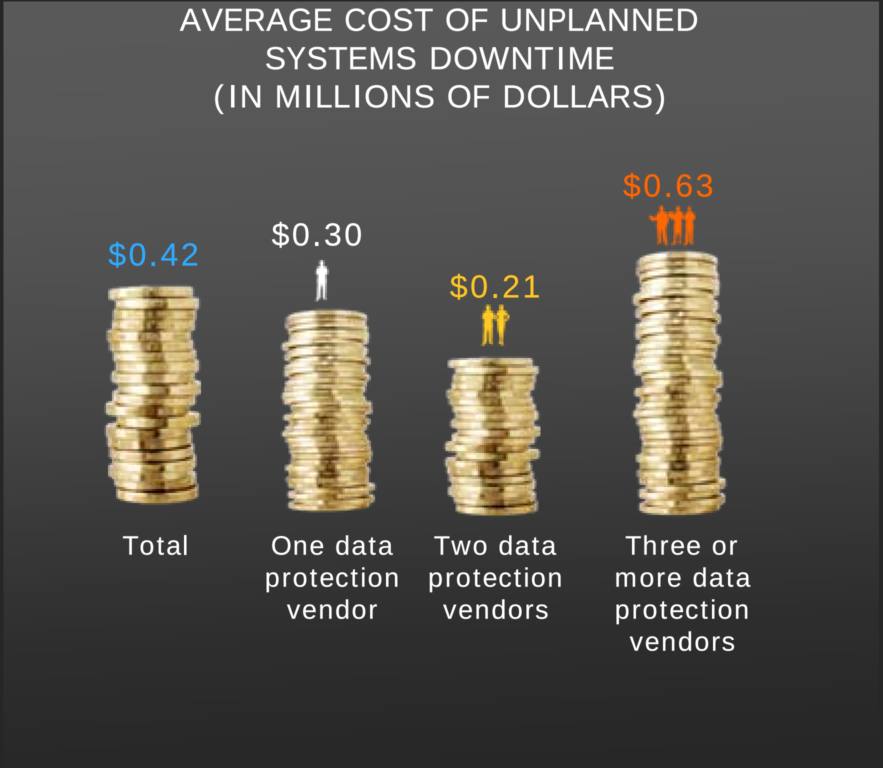
THE EFFECT OF THE NUMBER OF VENDORS ON DISRUPTIONS



- When a business has more than one vendor, they are more likely to experience unplanned systems downtime
- Around a third (32%) of those with three of more vendors have experienced data loss

Figure 10: Analysis of the organizations suffering disruptions, cut by the number of data protection vendors
Base: all respondents (125)

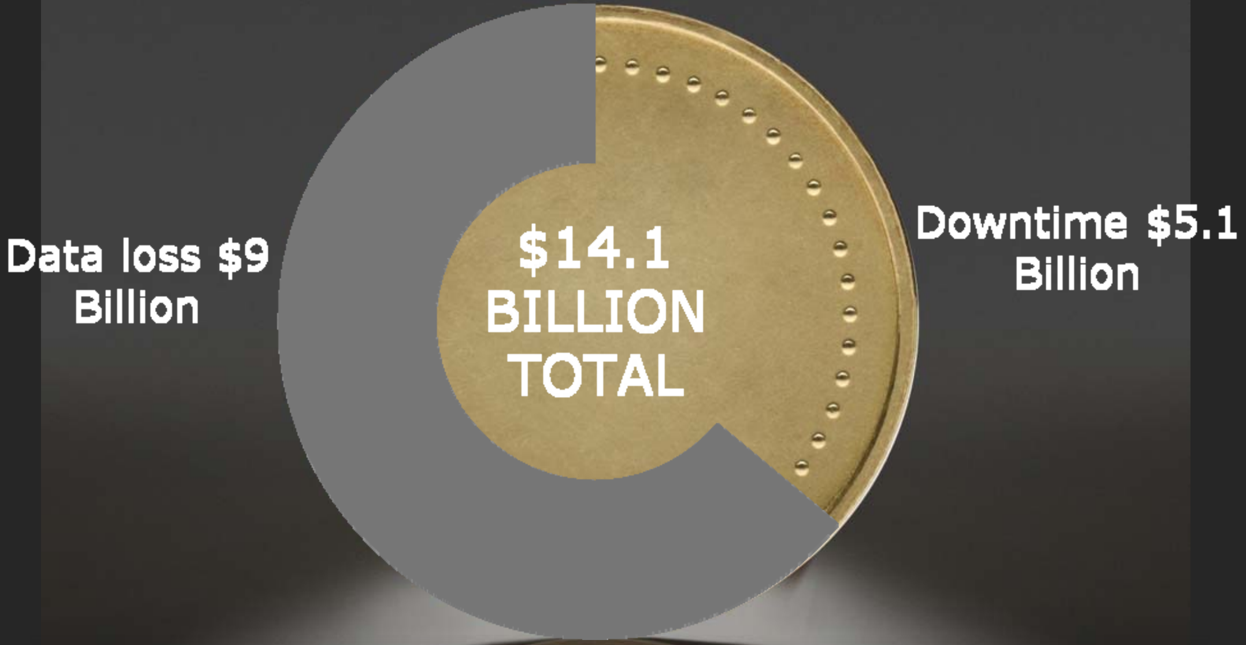
WHAT IS THE COST OF DOWNTIME?



- **26 hours** were lost on average over the last 12 months due to unplanned downtime, costing $0.42m
- This is similar to 2011 survey findings that had an average of **2 days** of downtime
- Organizations that have three or more vendors will lose more on downtime than those with two vendors

Figure 12: Analysis of the average cost of downtime, cut by number of data protection vendors
Base: respondents whose organization has suffered downtime (55)

ESTIMATED ANNUAL COST FOR DISRUPTIONS



FREQUENCY OF CONTINUOUS BACKUP

PERCENTAGE OF DATA BACKED UP CONTINUOUSLY BY BUSINESSES

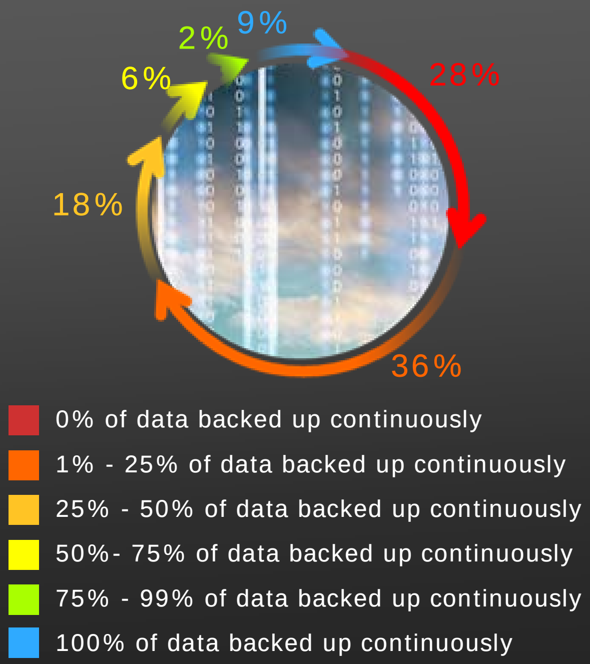


Figure 13: Analysis of those that backup data continuously
Base: all respondents (125)

- On average, a quarter of data is backed up continuously
- 83% of those “ahead of the curve” back up some data continuously, compared to 72% of Laggards

WHAT IS CAUSING THESE DISRUPTIONS?

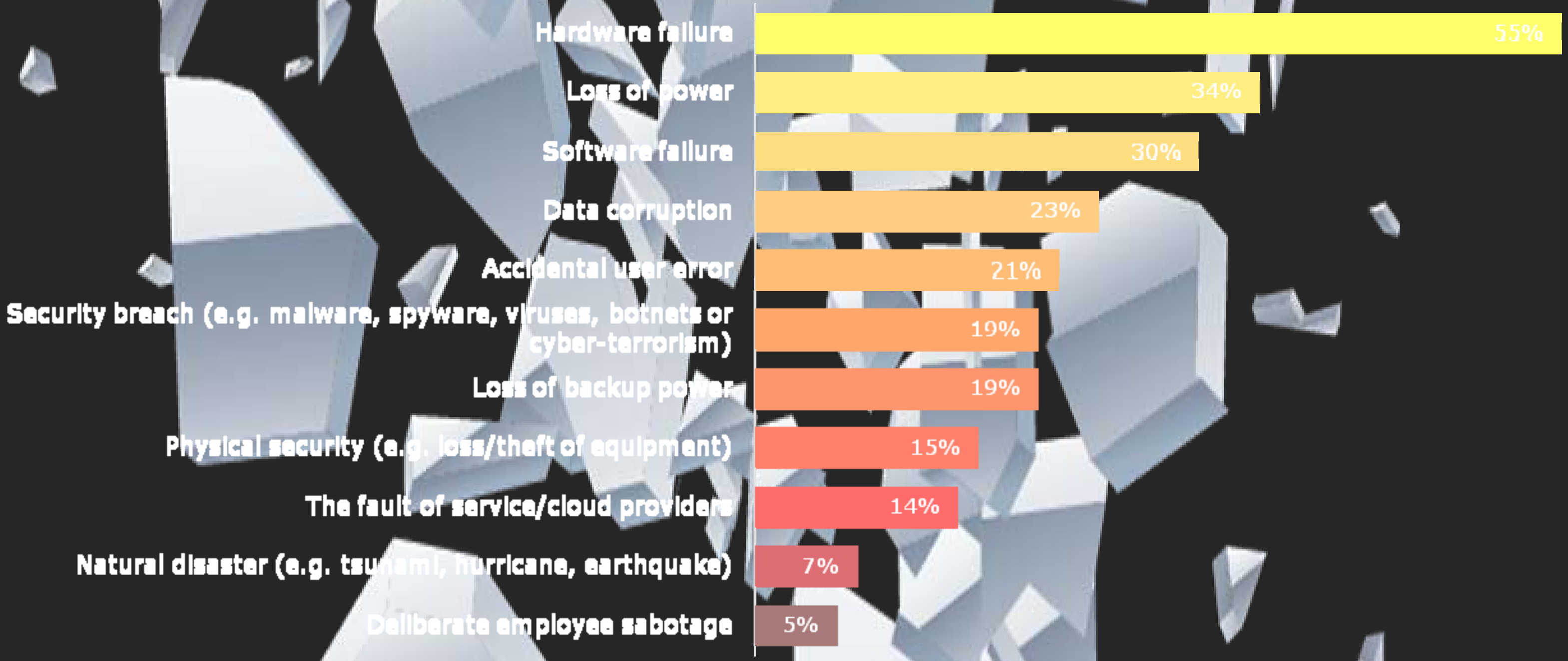


Figure 14: “What were the causes of your data loss and/or systems downtime?”
Base: respondents whose organization suffered data loss or downtime (73)

THE CONSEQUENCES OF DISRUPTION

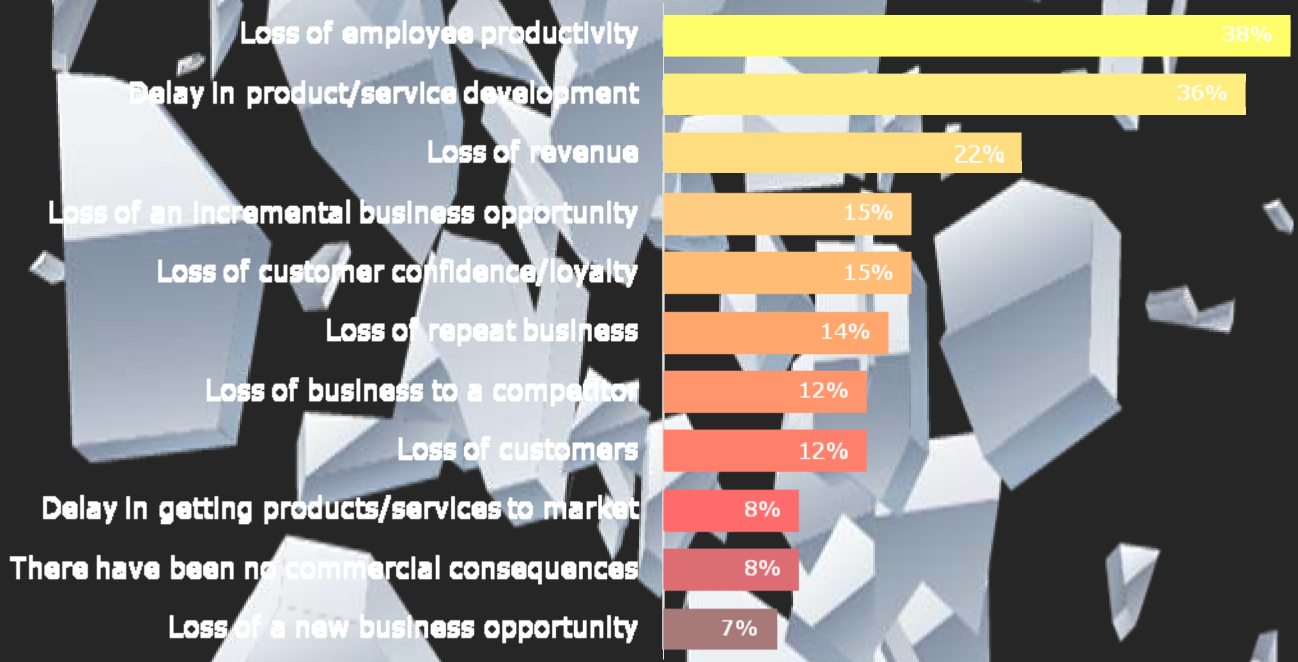
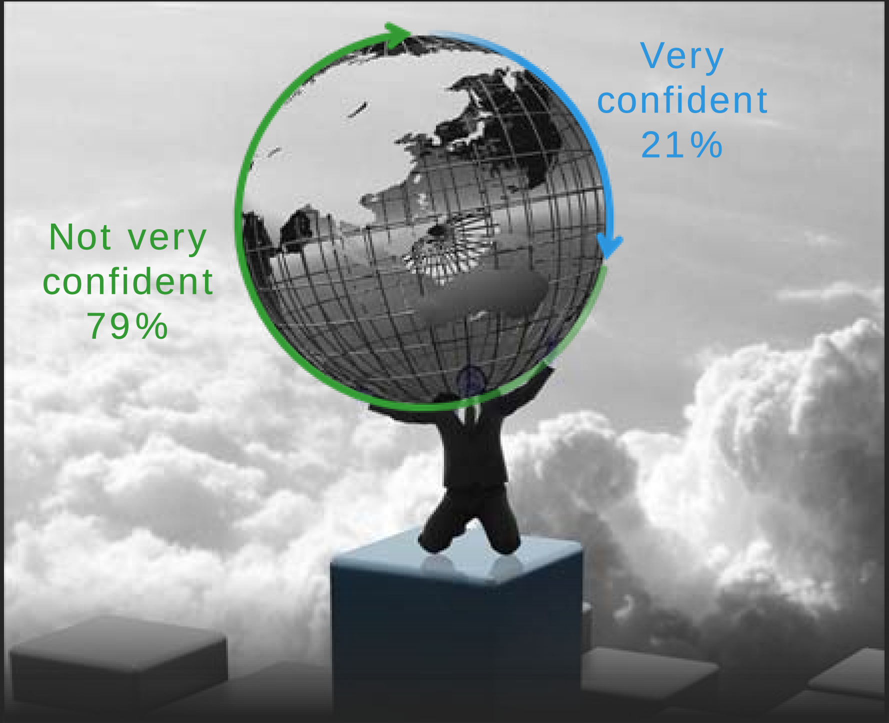


Figure 15: “Have any of the above been commercial consequences of the data loss and/or systems downtime you have experienced over the last 12 months?”
Base: respondents whose organization suffered data loss or downtime (73)

ARE ORGANIZATIONS CONFIDENT?



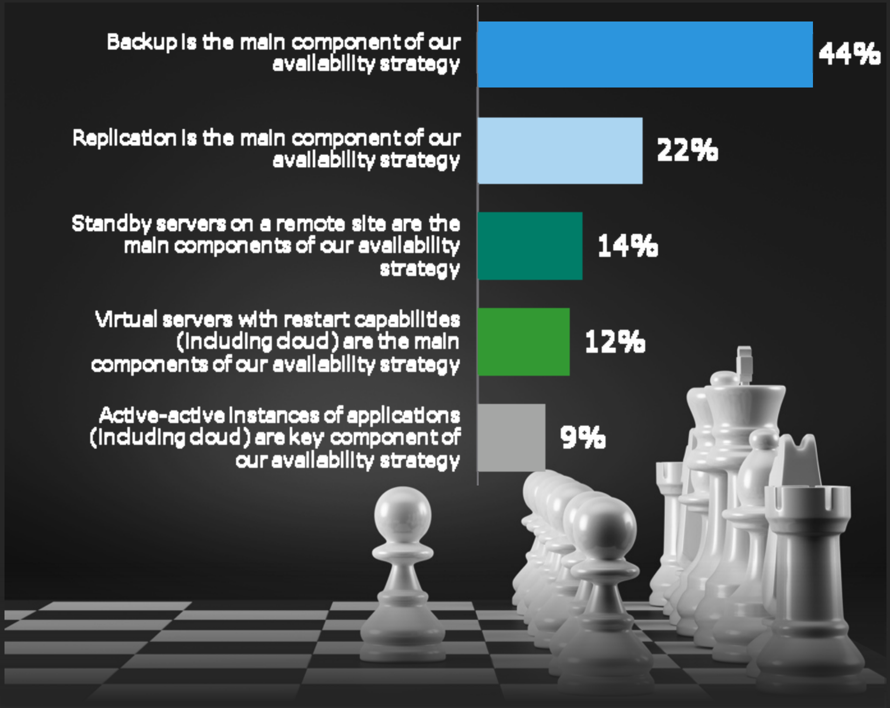
- 79% not fully confident that they can recover systems/data today from all platforms
- Only 7% from the manufacturing sector are very confident. Financial services is most confident (42%)

Figure 16: “How confident are you that, in the event of a data loss incident, you can fully recover systems/data today from all platforms, on-premise and off-premise, in order to meet business service level agreements?”
Base: all respondents (125)

Used for maturity matrix

DATA PROTECTION METHODS

WHAT STRATEGIES ARE IN PLACE?



- A significant proportion (44%) use backup as the primary protection strategy
- Only 9% use active-active as a key component
- Those with active-active as key component suffered less data loss than those with backup
  - 0% active-active vs. 24% backup

Figure 17: “Which of the above best characterises your organization's current data protection environment infrastructure?”
Base: all respondents (125)

Used for maturity matrix

WHAT OTHER STRATEGIES ARE IN PLACE?

THERE IS NO CONSENSUS ON THE TECHNOLOGY IN PLACE FOR AVAILABILITY, ALTHOUGH AN AVERAGE OF THREE STRATEGIES SHOWS A VARIED APPROACH ACROSS ALL ORGANIZATIONS

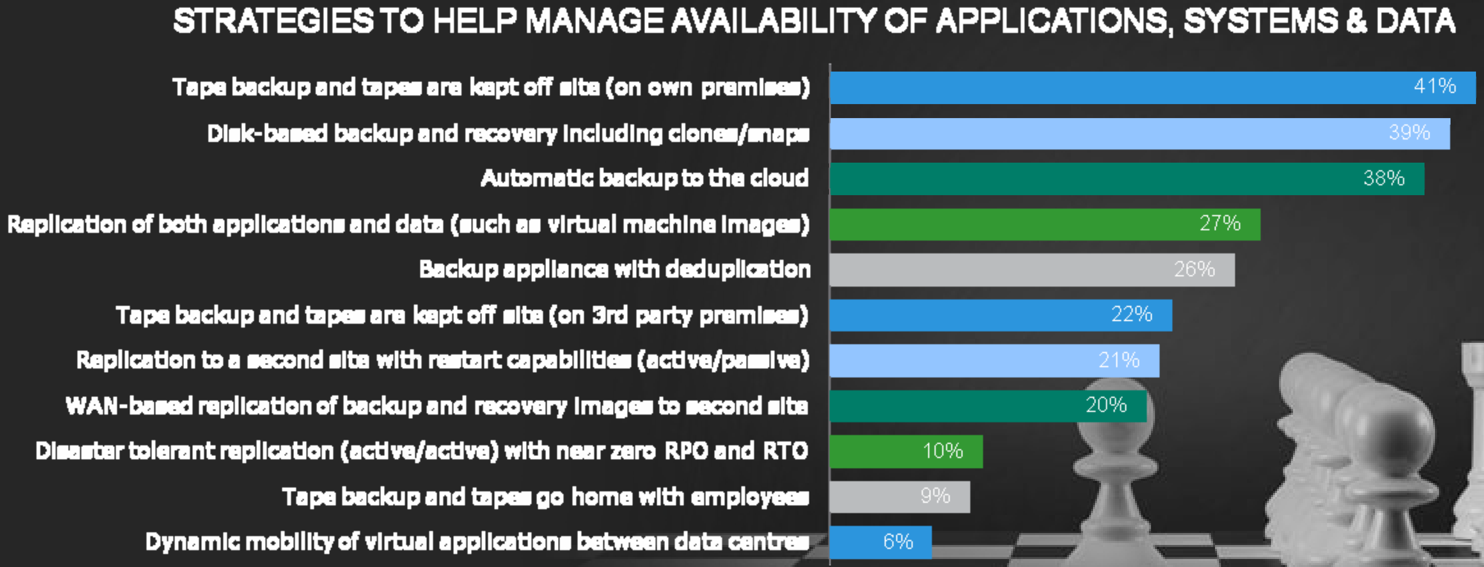


Figure 18: “Which technologies/strategies are in place to help you manage the availability of your applications, systems, and data?”
Base: all respondents (125)

Used for maturity matrix

WHO IS IN CHARGE OF THE CLOUD?

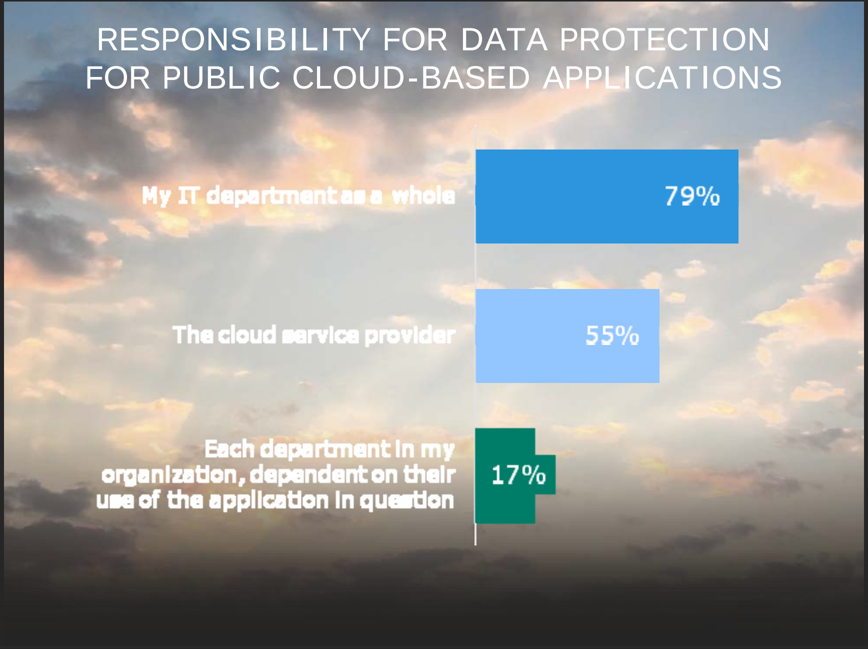

RESPONSIBILITY FOR DATA PROTECTION FOR PUBLIC CLOUD-BASED APPLICATIONS

Figure 19: “For public cloud based applications, which organizations are responsible for data protection?”
Base: respondents whose organization is using a type of cloud as a platform for infrastructure (75)

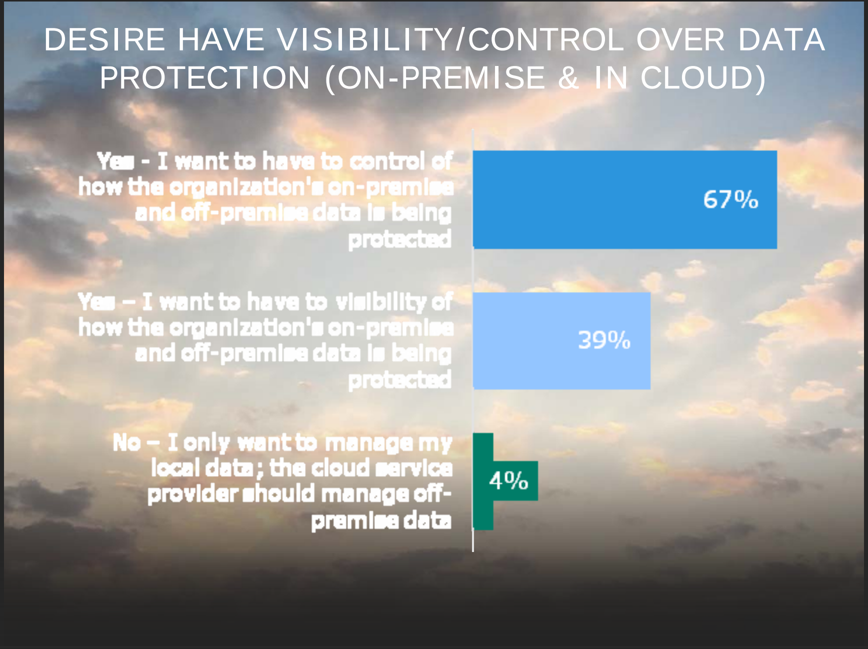

DESIRE HAVE VISIBILITY/CONTROL OVER DATA PROTECTION (ON-PREMISE & IN CLOUD)

Figure 20: “Do you want to have visibility and/or control over how your data is being protected both on-premise and in the cloud?”
Base: respondents whose organization is using a type of cloud as a platform for infrastructure (75)

WHERE IS DATA STORED?

PRIMARY DATA

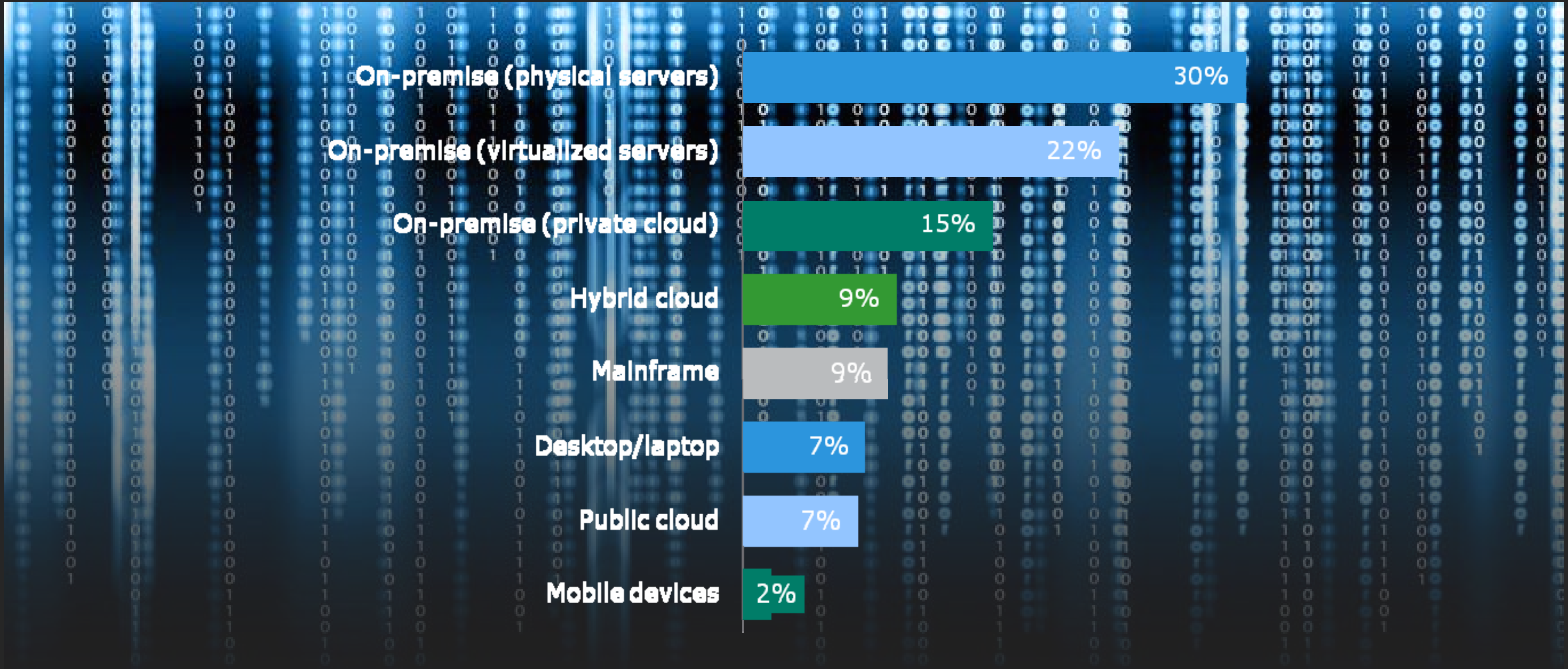


Figure 21: Analysis of average amount of primary data on different platforms
Base: all respondents (125)

WHAT IS HARDEST TO PROTECT?

MAJORITY DO NOT HAVE DISASTER RECOVERY PLAN FOR SOME APPLICATIONS THEY FIND HARDEST TO PROTECT

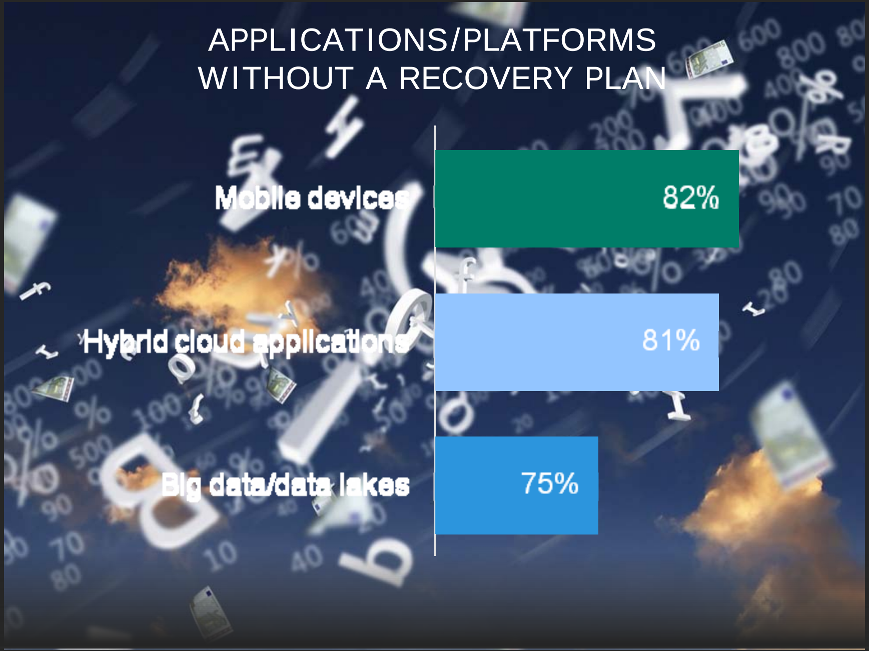


Figure 22: Analysis of applications/platforms that do not have disaster recovery plans
Base: all respondents (125)

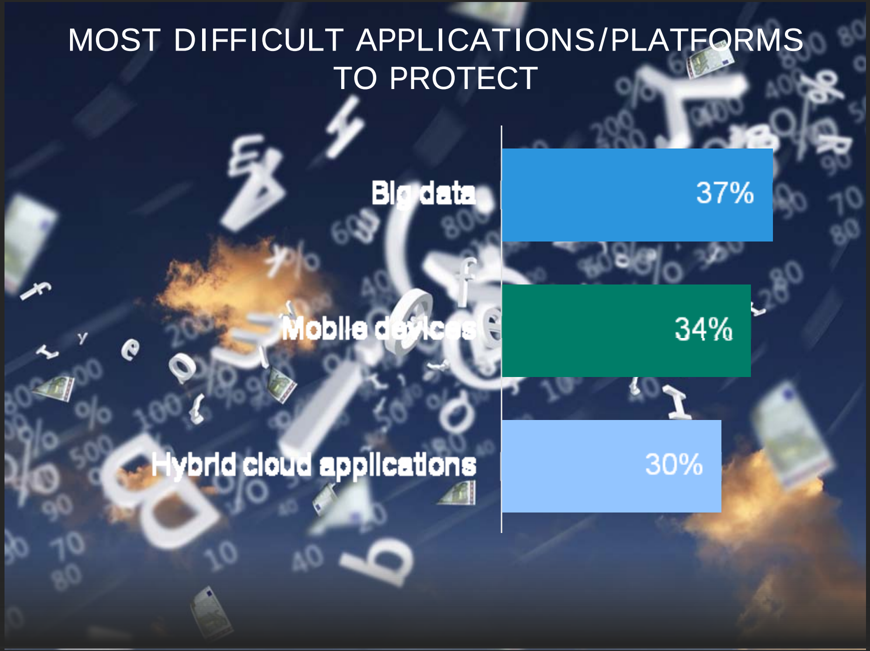
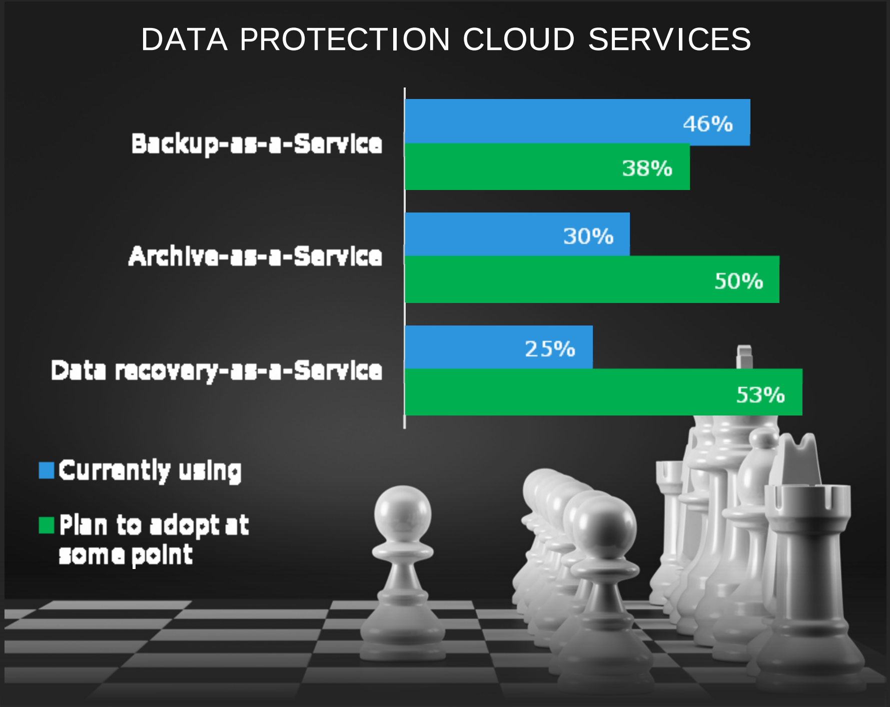


Figure 23: Analysis of applications/platforms that are difficult to protect
Base: all respondents (125)

FUTURE STRATEGIES



- 46% currently using Backup-as-a-Service; further 38% plan to in the future
- 50% plan to use archive as a service and 53% plan to use data recovery as a service in the future

Figure 24: “Are you currently, using or looking to adopt, any of the above data protection cloud services in the next 12 months?”
Base: all respondents (125)

SUMMARY FOR ITALY

ENTERPRISES ARE LOSING AS MUCH AS $14.1 BILLION THROUGH DATA LOSS AND UNPLANNED DOWNTIME

72% consider data protection to be critical to their organization's success, still **58%** suffered either downtime or data loss in last 12 months

More than one data protection vendor results greater loss of data when disruptions occur

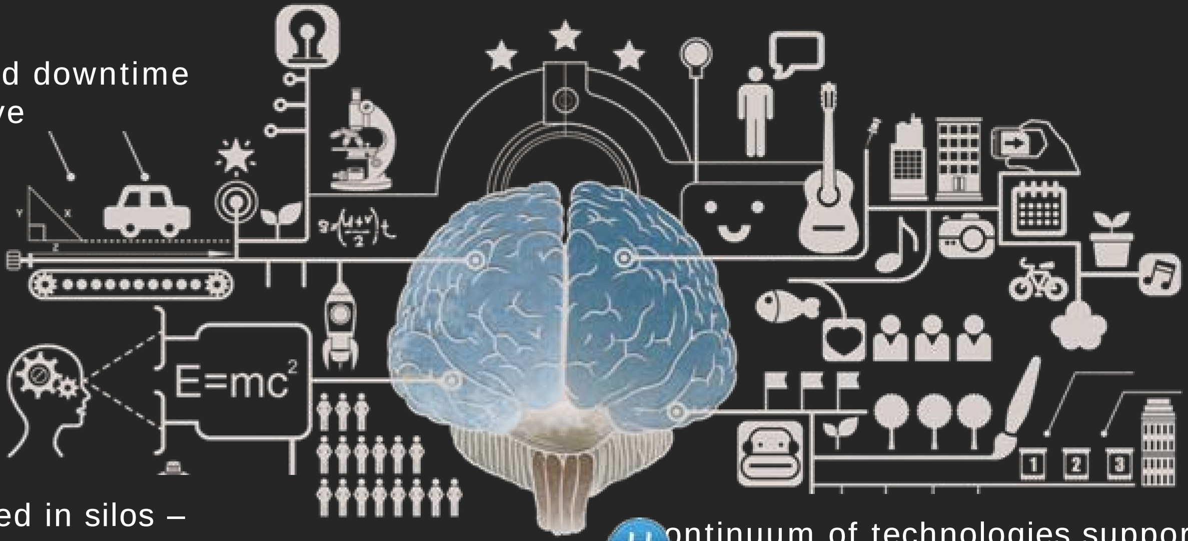
90% of businesses are behind the curve for data protection maturity and **79%** of businesses are not fully confident in their ability to restore apps/data

CONCLUSION

1 Data loss and downtime are expensive

2 Most companies globally are behind the curve and feeling pain

3 Newer workloads and exploding data volumes will continue to put pressure on data protection



4 ontinuum of technologies supports availability and protection requirements for different tiers of apps/data

5 s can’t be fixed in silos – isolated solutions by different vendors increase cost and risk

EMC RECOMMENDATIONS

- ✓ Make sure there’s an appropriate data protection solution in place for all of your critical data no matter where it is or how it is generated
- ✓ Manage an integrated data protection strategy and maintain a level of visibility and control for application owners
- ✓ Evaluate the gaps in your protection strategy that may emerge from disparate vendor solutions
- ✓ Match your data protection approach with the availability and protection requirements for your tiers of applications/data
- ✓ Understand who “owns” data protection – especially in the cloud

APPENDIX (i)

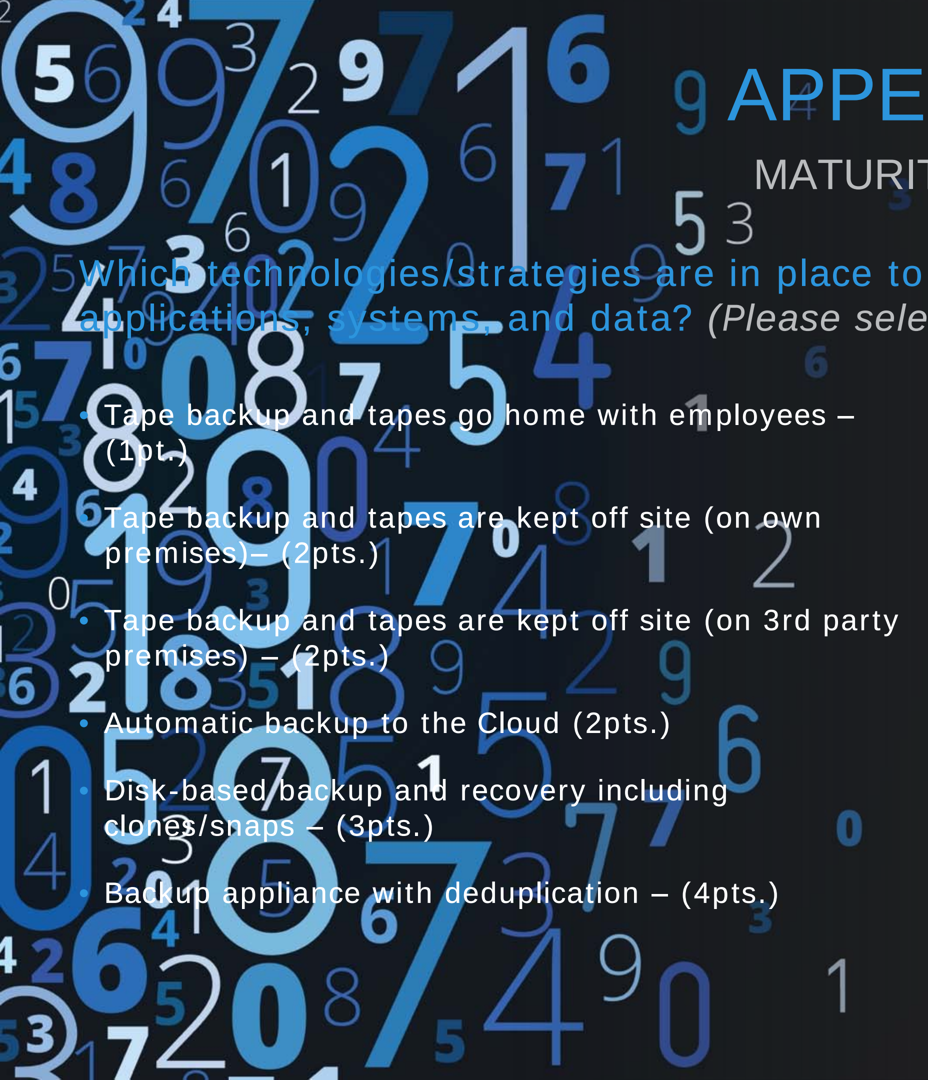
MATURITY SCORING

Which of the following best characterises your organization's current data protection environment infrastructure?

- Backup is the main component of our availability strategy – (1pt.)
- Replication is the main component of our availability strategy – (3pts.)
- Standby servers on a remote site are the main components of our availability strategy – (4pts.)
- Virtual servers with restart capabilities (including cloud) are the main components of our availability strategy - (5pts.)
- Active-active (two or more production data centres that are always on, 24/7 with no downtime) instances of applications (including cloud) are key component of our availability strategy – (6pts.)

What best describes your organization's archiving strategy?

- We don't have an archiving strategy – (0pt.)
- We use a backup application to archive data onto tape – (1pt.)
- We use an archiving application to archive data online (e.g. onto disk) – (3pts.)
- We use an archiving application to archive data to appliances that provide retention locking, litigation hold etc. – (5pts.)
- We use an archiving application to archive data to appliances that provide retention locking, litigation hold etc. and replicate/keep a copy off site - (7pts.)



APPENDIX (ii)

MATURITY SCORING

Which technologies/strategies are in place to help you manage the availability of your applications, systems, and data? *(Please select all that apply)*

- Tape backup and tapes go home with employees – (1pt.)
- Tape backup and tapes are kept off site (on own premises)– (2pts.)
- Tape backup and tapes are kept off site (on 3rd party premises) – (2pts.)
- Automatic backup to the Cloud (2pts.)
- Disk-based backup and recovery including clones/snaps – (3pts.)
- Backup appliance with deduplication – (4pts.)
- WAN-based replication of backup and recovery images to second site – (4pts.)
- Replication of both applications and data (such as virtual machine images) – (5pts.)
- Replication to a second site with restart capabilities (active/passive) – (5pts.)
- Dynamic mobility of virtual applications between data centres – (7pts.)
- Disaster tolerant replication (active/active) with near zero RPO and RTO – (8pts.)

APPENDIX (iii)

MATURITY SCORING

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

- Our recovery time is more than one working day (please specify) – (0pt.)
- Our recovery time is 12 - 24hours – (1pt.)
- Our recovery time is 6 -12 hours (2pts)
- Our recovery time is 3 – 6 hours (3pts)
- Our recovery time is 2 – 3 hours (4pts)
- Our recovery time is 1 – 2 hours – (5pts.)
- Our recovery time is less than an hour– (6pts.)
- Our recovery time is zero – (7pts.)
- I do not know – (0pt.)

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

- Very confident – (6pts.)
- Moderately confident – (4pts.)
- Some doubt – (3pts.)
- Not very confident – (1pts.)
- Not at all confident – (0pts.)

EMC^{2}®