

PROTECTING DATA CAPITAL IN YOUR ORGANIZATION

eBook

executive summary

The digital era is changing the way that organizations think about, protect, and monetize data.

Now more than ever they are pushing to be *digitally-driven*, and to achieve this they must be *data-driven*.

Data powers everything in modern organizations; analytics, digital experiences, IoT, and artificial intelligence are notable examples. All are essential to organizations that want to succeed in a digitally transformed world, but they simply cannot function without data. **This is driving the shift from data as a static digital asset to data as a strategic business asset.**

Those who do not invest in sufficient *data protection* risk limiting their success in these key areas.

This eBook presents findings from Vanson Bourne's Global Data Protection Index study, a survey of 2,200 IT decision makers (ITDMs) globally

Contents:

	Macro trends	3
	A deep dive into data capital	5
	Why is effective data protection so difficult?	7
	Global Data Protection Index findings	8
	Top 6 qualities of a data protection leader	9
	Summary	10

macro trends: the changing data protection landscape

Data holds considerable value.

Our research found that in the vast majority of organizations this value is recognized and, in many cases, organizations are starting to actively monetize data:

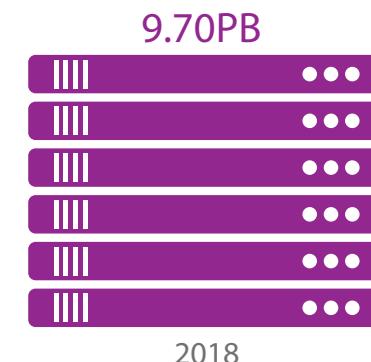
92% see the potential value that data holds

36% treat data as extremely valuable and are currently monetizing it

As a result, organizations have more data under management than ever before. Over time, the quantity of data will continue to grow exponentially as the attitude of treating data as capital becomes more widespread.

As organizations continue to realize the importance of data and begin to treat it as an asset, data storage and protection becomes increasingly important.

Total volume of data managed, 2016 vs. 2018





What does the valuation of data mean for the importance of data protection?

As the value of data increases, so does the financial cost that faces organizations if they suffer a disruptive event, such as unplanned systems downtime or data loss.

In the last 12 months alone, over four in ten (41%) have experienced unplanned systems downtime, costing an average of \$527,000 USD and almost a third (28%) have experienced data loss, costing an average of \$996,000 USD.

Disruptive events, such as unplanned systems downtime, data loss, and ransomware attacks are problems that many organizations struggle to defend against.

Therefore, a comprehensive data protection plan needs to be in place to ensure that if disruptive events do occur, organizations are in a position where they can quickly and effectively recover all of their high-value data.

In the last 12 months...

41%

have experienced **unplanned systems downtime**, costing an average of **\$527,000 (USD)**

28%

have experienced **data loss**, costing an average of **\$996,000 (USD)**



a deep dive into data capital

What is data capital?

Data capital refers to any wealth or value that has been derived through using an organization's data.

As well as having value in its own right, data is crucial to digital transformation and plays an important role in allowing existing assets and infrastructure to unlock new, previously untapped value.

The digital era that organizations now find themselves in means that **unprecedented data growth is unavoidable**. Next-generation technologies and workloads (e.g. IoT, AI) in particular are at the heart of many organizations' digital

transformation plans, and they create significant quantities of data and amplify this growth.

This is leaving many organizations in need of a rethink – as seen below, almost half currently do not have data protection solutions in place that will be suited to their future data protection needs:

45%

of ITDMs say that one of the top three data protection challenges facing their organization is a lack of solutions for new, data-rich technologies

Next-generation technologies and workloads that are powered by data



Analytics



Digital UX



IoT



AI



Given the magnitude of macro changes, the way that organizations treat and protect data must also change.

Data protection can no longer be an afterthought for organizations. As the potential to monetize data grows, so does the risk associated with not protecting it properly. And this is not limited to high costs associated with data loss and unplanned downtime; 19% of those who experienced data loss and/or systems downtime in the past 12 months also lost customers as a result.

In the past, many organizations would choose to take out an insurance policy that would cover them for any expenses or liabilities that came as a result of a disruptive incident, but this is no longer a sufficient approach – this does not cover for the most important and valuable asset of them all – the data.

A bold prediction for the future:

Data protection will no longer just be about safeguarding data. Instead, **data protection will play the role of protecting and extending the value of that data** over time, ensuring that data is available and accessible as needed.



why is effective data protection so difficult?

The importance of implementing more effective data protection is clear, but there are three key challenges that make data protection difficult for organizations:



① Managing complex data footprints

The data landscape has become highly complex as a result of mergers and acquisitions, different data storage and management processes, determining what is stored on-premises vs. cloud, and so on.



② Keeping up with data growth

Organizations are now handling more data than ever before, and the trend is set to continue at a near-exponential rate. Organizations must be able to back up and store it all effectively but this is becoming an increasingly difficult task.



③ Continuously safeguarding data

As data value grows, so do the costs of a disruptive event such as downtime or data loss. The importance of recovering quickly from these events is higher than ever.

Many organizations are also trying to juggle multiple data protection vendors while facing these challenges. However, findings from this research highlight that those with multiple vendors are more likely to experience data protection-related disruption.

global data protection index findings

Vanson Bourne's Global Data Protection Index research categorized 2,200 respondents' organizations into **four maturity groups** in terms of data protection:

Data protection **Leaders**
Data protection **Adopters**
Data protection **Evaluators**
Data protection **Laggards**

Organizations were grouped based on their maturity in terms of a number of important elements relating to data protection, including:

- Backup and recovery confidence
- Data protection strategy and infrastructure
- Value placed on data



Explore the full GDPI results at DellEMC.com/GDPI

the top 6 qualities of a data protection leader

By analyzing the data protection maturity model we can create a persona for organizations that are classified as **Data Protection Leaders**. They:

- ① Place **greater value on data** (i.e. are more likely to be monetizing data)
- ② Make **better use of public cloud** to improve their data protection
- ③ Have **shorter recovery times** after unplanned systems downtime
- ④ Have **more future-proof** data protection solutions
- ⑤ Are **more compliant** with data governance regulations
- ⑥ Are well-equipped to recover **all business critical data** and do so **from all systems and platforms** in the event of cyberattacks or other data loss incidents

All modern organizations should be striving to reach Leader status, but to do so they must be improving and future-proofing the data protection solutions they have in place. In order to truly realize the value data can bring to an organization and to effectively leverage that data in a way that can bring real business benefits, organizations need to work on the above areas and push towards Data Protection Leader status.



summary

With organizations managing a greater volume of data than ever before and the concept of data capital becoming increasingly embraced by organizations, the importance of innovative and modernized data protection has never been higher.

In the digital future, data protection will become one of the most critical areas where investment is required. Organizations who do not have comprehensive data protection in place may limit their ability to get sustained value from their data over time.

Looking to the future...

Organizations need to stop treating data protection as an insurance measure (a 'just in case') and instead **start to view it as a business-enabler** and a way of safeguarding one of their greatest assets – their data.

Volume of
managed data
is increasing



Value assigned
to data is
increasing



Importance of
data protection
is increasing



What your organization should be doing to maximize the value of its data:

- 1 Centralize data protection strategy and make it a board-level initiative
- 2 Assign value to data that your organization manages
- 3 Consolidate vendors – multi-vendor strategies are adding unnecessary risk
- 4 Utilize a multi-cloud approach where appropriate to lower data protection costs
- 5 Invest in future-proof data protection solutions

Become a Data Protection Leader with Dell EMC

VansonBourne

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis, is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com

About Dell EMC

Dell EMC, a part of Dell Technologies, enables organizations to modernize, automate and transform their data center using industry-leading converged infrastructure, servers, storage and data protection technologies. This provides a trusted foundation for businesses to transform IT, through the creation of a hybrid cloud, and transform their business through the creation of cloud-native applications and big data solutions. Dell EMC services customers across 180 countries – including 99 percent of the Fortune 500 – with the industry's most comprehensive and innovative portfolio from edge to core to cloud.

Commissioned by Dell EMC