DATA PROTECTION IN THE FOURTH INDUSTRIAL REVOLUTION

In today's hyper-competitive market, organizations can't afford to be offline. Whether a mid-size company in the manufacturing industry, a multinational healthcare company, or a Fortune 500 retail giant, business doesn't stop when the clock strikes five.

We now live in an experience economy, where customer loyalty is driven by convenience. No longer can organizations depend on product quality to boost the bottom line; for most, product quality is not only a given. It's expected.

Today, organizations must deliver what the customer wants, when they want it. And let's face it – everyone, regardless of industry, expects instant access to information and the ability to buy products or services anytime, from anywhere.

So, what's the one "thing" that facilitates this convenience – the positive experience that is now the hallmark of customer loyalty? The IT organization.

A Study of Our Experience Economy

> **It's a fairly obvious observation that our new world is data-driven. Over half of the Fortune 500 have disappeared since the year 2000, simply because they didn't embrace the realities of modern digital business.[1]**

Some call this the Fourth Industrial Revolution, with the introduction of the digital consumer and subsequent optimization of business. Those that didn't embrace this digital transformation have ceased to exist.

Not surprisingly then, an organization's most critical asset has become its data; and, protecting it is arguably the single most important factor in its ability to thrive. To gain more insight into how organizations are modernizing their approach to handle new data types, increased workload volumes and meet rising service level agreements (SLAs), Arcserve commissioned independent research firm MayHill Strategies to survey IT decision makers around the world.

This study was conducted in September of 2018 via online interviews with 759 individuals in the United States (N=253), United Kingdom (N=251) and Germany (N=255) who self-identified as being completely responsible or involved in IT decisions for their organization. Weights were applied by industry and job responsibility to ensure a balanced sample.

Media Scaremongering Fuels Concern Over Data Safety

If you thought scare tactics were only effective in political ads, the truth is news media is just as impactful at increasing concerns about data safety. According to new research, 58% of IT decision-makers identified recent coverage of data breaches and ransomware attacks as a key concern relative to their ability to safeguard business-critical data. This apprehension is certainly justified, with a ransomware attack estimated to occur every 14 seconds by the end of 2019[2]. Yet, even with ransomware being a real concern for 91% of IT decision makers, nearly 70% still view the threat as a data security – not recovery – issue.

But it doesn't stop there. Media coverage of Facebook's recent data breach also sparked fear for 42% of IT decision makers – more so than a digital disruption to their own business applications and systems, or recent natural disasters.

To prepare for and mitigate threats of events such as cyber-attacks and system outages, 89% of IT decision makers indicate having a formal disaster recovery plan in place. What's alarming is nearly 75% aren't fully confident in their ability to recover business-critical data in time to avoid a disruption in business. The obvious question is why.

The answer lies in the high costs and time required to protect multi-generational infrastructures ranging from non-x86 and x86, to software as a service (SaaS) and infrastructure as a service (IaaS). In fact, 64% of IT decision makers agree that protecting business-critical data has not become easier over the past five years despite efforts to simplify and reduce costs.

MODERN IT IS MULTI-GENERATIONAL

IT decision makers rank their most-used backup methods:

36% D2D2C
Backup to disk, then data moved to cloud

16% D2D2D
Backup to disk, then data moved to lower tier disk

13% D2D2T
Backup to disk, then data moved to tape

17% D2C
Back up directly to cloud

14% D2D
Backup to disk

3% D2T
Backup to tape

Decision Makers Are Divided: Speed of Recovery or Loss of Business Activity

Most IT decision makers agree that safeguarding business-critical data has become more difficult, primarily due to resource constraints, high costs and multiple backup tools needed to protect complex infrastructures. Fifty-one percent of survey respondents cite the amount of time and skill required to keep backups functioning and the high expense of backup solution acquisition and support equally as challenging; however, C-class executives were significantly more likely to state cost as the most difficult aspect to safeguarding data. The need for separate and/or additional backup tools to support new workloads, and more frequent recovery points, were named by nearly half of IT decision makers as key challenges of protecting data.

Yet, as backup infrastructures are clearly becoming more costly and complex, the tolerance for data loss is diminishing.

> **Ninety-three percent of IT decision makers revealed their organizations could tolerate "minimal," if any, data loss from critical business applications, with half saying they have less than an hour to recover business-critical data before it starts impacting revenue.**

However, IT decision makers are divided on the importance of recovery speed versus the extent to which business activity is lost, with only half stating both are of equal importance in recovery efforts. Significantly, a quarter of respondents indicate the speed of getting back online is of more importance than how much data they actually lose, despite very few stating their business could withstand more than eight hours of business inactivity. So, why the disparity?

For many, aligning recovery time and point objectives (RTOs/RPOs) is perceived as too costly and unachievable for all but the largest of enterprises. However, it can be argued that this perception is becoming a bit dated – particularly with the rise of cloud-native backup and disaster recovery as a service (BaaS/DRaaS) solutions that bring value and affordability to those who require both RTOs and RPOs of minutes. This balance between the cost of disaster recovery and the impact of an outage is one all organizations must carefully address.

Not All Clouds Are Created Equal

Cloud is rapidly changing the way businesses back up data, with an estimated 83% of IT workloads running in the cloud by the year 2020[3]. Digitally transforming enterprises is the leading factor of public cloud engagement today; however, most say security is the biggest concern in adopting a cloud computing strategy. IT decision makers in our survey agree, stating a move to the cloud is their top priority this year. They also cite security as a concern, but interestingly, not necessarily with private clouds.

> **When asked to compare the security of business-critical data in a variety of storage types, IT decision makers believe private clouds to be *more* secure than local storage, blockchain, hypervisors and public clouds.**

In fact, IT decision makers are two times more likely to believe private clouds are completely secure. Perhaps this is caused by high-profile public cloud security breaches, or quite possibly because most major public cloud vendors don't provide SLAs beyond 99.99% - translating to almost one hour of downtime a year and losses of $500,000 USD for a company with $1 billion in revenue.

Response time is also varied and not guaranteed. For example, an organization using public cloud for disaster recovery can expect to wait approximately 15 minutes for response to a critical case and one hour for urgent cases. So, while the move to the cloud continues, organizations must be vigilant about incorporating cloud workloads, including data in IaaS and SaaS, into their data protection strategies.

Barriers of Emerging Technologies

Originally invented in 2008 for cryptocurrency bitcoin, blockchain technology has taken the tech community by storm as other potential uses have emerged to create permanent, public ledgers for everything from smart contracts and banking to tracking sales data and music distribution. But while some companies have hopped on the blockchain bandwagon, the overwhelming majority of IT decision makers from our research state they aren't currently using this technology; a position also found by recent Gartner research that reports only 1% of CIOs indicate any kind of blockchain adoption within their organizations.[4]

There are a variety of reasons blockchain hasn't been rapidly adopted, ranging from unfamiliarity with the technology itself to how, and if, it should be safeguarded. Only 35% of IT decision makers in our survey cite being very familiar with blockchain; however, of those that are, C-class executives say they are much more so than mid-IT management.

On the other hand, solutions powered by artificial intelligence (AI) are much more widely accepted by IT decision makers in our research, with nearly 75% citing awareness of "intelligent" data recovery solutions. Based on what respondents know or have heard, the vast majority are likely to consider AI-driven solutions, particularly in the US and UK where nearly 90% of IT decision makers say they are somewhat or very likely to consider these technologies. However, despite the interest in backup and recovery solutions that incorporate AI, only one in three report a great deal of trust in the vendors that offer them. Why? Awareness of newer technology doesn't readily translate into acceptance, and perhaps many are skeptical of claims that aren't backed by results.

Nevertheless, AI-powered backup and recovery opens a new frontier for digital business and promises to extend the reach of IT decision makers far beyond data protection.

THE AI-POWERED WISH LIST

IT decision makers identify their top priorities for intelligent backup and recovery solutions:

1. Proactively replicate data to the cloud before a downtime event or disaster occurs
2. Intelligently provide visibility into the entire backup IT infrastructure
3. Intelligently restore the most frequently accessed, cross-functional or critical data first
4. Model and test different disaster and recovery scenarios

Conclusion

The way we perceive and interact with technology to manage and protect the lifeblood of every organization has, historically, been a critical factor in business viability; and, will continue to facilitate a radical transformation. Global coverage of data breaches and ransomware attacks isn't going away, however the necessary shift in mentality to these events being a recovery issue may mean more organizations won't fall victim to data loss and downtime that often occur as a result.

> **Not surprisingly, the business of backup and recovery is getting more complex with modern IT being less about siloed business and IT priorities, but rather the inseparable link between the two.**

Solutions are needed to resolve widespread resource constraints and high costs associated with managing and protecting data proliferation. And while cloud sits at the forefront of IT priorities for these reasons, most IT decision makers still must contend with alternate platforms – effectively making modern IT multi-generational.

But when it comes to protecting multi-generational infrastructures, IT decision makers are divided between what's more important: the speed of recovery or the amount of data their organization is willing to lose. The overwhelming majority reveal they have less than an hour to recover before revenue is impacted and can tolerate "minimal," if any, data loss – yet just a quarter feel extremely confident in their ability to recover quickly enough to avoid business disruption. What if these organizations didn't have to choose?

As IT decision makers look at methods to balance the costs of disaster recovery and the impacts of an outage, many will look to private clouds to mitigate the hidden costs and perceived security risks of public cloud platforms. Once the tale of science fiction, emerging technologies such as new uses of blockchain and AI-powered backup and recovery solutions will only accelerate opportunities for IT decision makers to deliver capabilities beyond data protection.

About Arcserve

Arcserve provides exceptional solutions to protect the priceless digital assets of organizations in need of full scale, comprehensive data protection. Established in 1983, Arcserve is the world's most experienced provider of business continuity solutions that safeguard multi-generational IT infrastructures with applications and systems in any location, on premises and in the cloud. Organizations in over 150 countries around the world rely on Arcserve's highly efficient, integrated technologies and expertise to eliminate the risk of data loss and extended downtime while reducing the cost and complexity of backing up and restoring data by up to 50 percent. Arcserve is headquartered in Minneapolis, Minnesota with locations around the world.

SOURCES

[1] Digital Disruption Has Only Just Begun. World Economic Forum. Retrieved 10/25/2018.

[2] Global Ransomware Damage Costs Predicted To Hit $11.5 Billion By 2019. Cybersecurity Ventures. Retrieved 10/26/2018.

[3] 83% Of Enterprise Workloads Will Be In The Cloud By 2020. Forbes. Retrieved 10/26/2018.

[4] "Hype Killer - Only 1% of Companies Are Using Blockchain, Gartner Reports | Artificial Lawyer". Artificial Lawyer. 2018-05-04. Retrieved 10/26/2018.

Explore more at **arcserve.com**

Copyright © 2018 Arcserve (USA), LLC and its affiliates and subsidiaries. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective owners. This document is for your informational purposes only. Arcserve assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, Arcserve provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will Arcserve be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if Arcserve is expressly advised in advance of the possibility of such damage.