arcserve®

# State of Data Resilience in the Enterprise

Peer insights and thought-provoking ideas to assess and improve your organization's data resilience

**Independent Research Commissioned by Arcserve**

Executive Summary

# Foreword

Data resilience has become crucial to the very survival of most organizations today, and your organization is likely no exception. With the explosive growth and proliferation of AI-powered tools, your risk of suffering a ransomware attack or a data breach keeps increasing as cybercriminals find new ways to outsmart or overcome your frontline cyber defenses. Even the Federal Bureau of Investigation (FBI) recently warned about the increasing threat of cyber criminals leveraging artificial intelligence to increase "cyberattack speed, scale, and automation.[1]"

At the same time, more businesses are embarking on their own AI initiatives – maybe yours is, too. Such projects almost always require massive amounts of proprietary data and come to a standstill if that data is lost or stolen. Then, once model training finishes, the training data must still be preserved for governance and compliance purposes (e.g., to support an anti-bias audit of model predictions).

Meanwhile, all the "legacy" risks to your data are still here: malicious actors (especially with remote work), accidental user error, natural disasters, and so on.

**97%**
**of survey respondents agree that their proprietary data is "moderately" or "extremely" critical to their company's success.**

**69%**
**of respondents said their organization's business operations would come to a halt if it lost access to its data.**

Arcserve commissioned a study of senior IT professionals directly involved with data backup and security to better understand how small- and medium-sized organizations deal with these evolving challenges. We are excited to share our findings with you and some of our thoughts on mitigating the risks of data loss and downtime.

We hope this perspective of your peers' data protection challenges and how they react to them helps inform your thinking as you assess your organization's data resilience strategy and its potential gaps. It may even help back up (pun intended) your recommendations to internal stakeholders.

## Team Arcserve

1 FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence. May 8, 2024

# Executive Buy-In Matters. 1 in 4 Don't Have It Yet.

Implementing the best data protection and cybersecurity practices with effective technologies requires IT and other investments. Buy-in from the leaders who hold your company's purse strings is indispensable.

Too many business leaders still don't prioritize data resilience, and our anecdotal evidence supports this finding. In conversations with small and medium-sized companies, we hear things like, "We're too small to get hit." The harsh reality is that they're not. When they do "get hit, " they're probably too small to make the news.

A successful data resilience initiative starts at the top, with buy-in from business leaders and the board of directors. But, like any change initiative, it needs support and cultural buy-in from the whole company, from the corner office to the front lines, across all departments. It also requires alignment and commitment from partners and service providers.

**25%+**
**of survey respondents couldn't say that their company's leaders worry about taking proper care of the organization's data.**

**and yet ...**

**69%**
**of survey respondents said their organization's business operations would come to a halt if it lost access to its proprietary data.**

The Cybersecurity & Infrastructure Security Agency's publication, "Making a Business Case for Security,"[2] offers helpful advice for gaining executive buy-in.

# Data Protection Investments Grow

Respondents said their IT organization already invests a substantial amount of their IT budget in data protection and recovery.

The high standard deviation (21%) among answers, however, supports the finding above that a substantial number of companies arguably vastly underinvest in this area. Presumably, smaller overall IT budgets impose difficult tradeoffs upon IT leaders.

The following data point offers some reassurance: overwhelmingly, IT leaders aim to grow their data protection budget.

**22%**
**the average portion of the survey respondents' organization's IT investment budget allocated to data protection and recovery.**

**89%**
**of survey respondents' organizations expect to increase their data protection budget in the future.**

They may find the 2023 Security Budget Benchmark Report helpful, as it showed that the average IT security budget increased by 6%. Overall, that's a pace of growth that's 65% slower than previously.[3] In many cases, though, growth must accelerate in the data protection bucket.

**Even as an increased budget gets allocated to data protection, how can an organization make the most of it?**

It is important to consider the tradeoffs between having a disparate patchwork of individually configured fine-tuned components and an integrated, unified solution that reliably gets the job done. The former may give you unique customization opportunities, while the latter should be easier to deploy and faster to deliver value.

2 Making a Business Case for Security I An Interagency Security Committee Best Practice. 2023 Edition
3 2023 Security Budget Benchmark Summary Report

# Data Recovery and Business Continuity

## Part 1: Time Is of the Essence

**What would the costs—in money and reputational damage—be if your business couldn't access its data?**

Here are some indications from reputable sources:

**Only 31%**
**of survey respondents are confident in their ability to recover lost data in 24 hours.**

### Financial risks

- **$2.7M**: average ransomware recovery cost, not counting ransom payments (Sophos State of Ransomware 2024)
- **$2M**: average ransom payment, +50% YoY
- **$9,000/minute**: average cost of downtime for large organizations (Forbes)
- **$5M / hour** for high-risk organizations (finance, healthcare)
- **$4.4M:** average cost of a data breach in 2023

### Compliance risks

- **US:** Data Privacy Act, CCPA
- **Europe:** GDPR
- **Japan:** Act on Protection of Personal Information

### Reputational risks

- Damaged relationships with customers, partners, and stakeholders

**Is taking more than 24 or 48 hours to recover acceptable for companies?**

We asked that question, and the answer was a resounding no for two out of every three companies.

**Only 34%**
**of survey respondents say their organization can take more than 48 hours to recover its data and still avoid significant business disruption.**

## Part 2: Practice Makes Perfect Ready

While the good news is that most organizations (70%) said they perform weekly or monthly data recovery drills, over one in five businesses don't test their systems often enough.

**70%**
**of survey respondents say their business performs weekly or monthly data recovery drills to ensure business continuity.**

Regular data recovery drills are essential because they help ensure that the organization's Recovery Time Objective (RTO) and Recovery Point Objective (RPO) can be met when disaster strikes.

# Legacy Risks: Hard Lessons Learned, for Many. Overconfidence, for Some?

Many IT leaders that we've spoken to are seasoned veterans. They've seen this movie before, and they've seen the risks materialize.

Nearly half of those surveyed responded “yes” when asked if they had experienced significant revenue loss due to data loss incidents.

**47%**
**of survey respondents say their organization has experienced significant revenue loss due to data loss incidents.**

Ponder this finding and its impact on organizational leaders. For those laser-focused on growing revenue and controlling costs, this revenue downside perspective should be a wake-up call. But it was no surprise to hear the respondents express confidence in their posture:

Overwhelmingly, the IT leaders that we spoke to say they are confident in their ability to detect and recover from threats to their data from legacy risks like insider threats and natural disasters.

**86%**
**of survey respondents say their organization is either “very” or “extremely” confident in their ability to detect and respond to natural disasters.**

Indeed, the 2024 Verizon Data Breach Investigations Report (DBIR) found that **25 percent** of breaches involved users from within the organization.[4] Meanwhile, according to the NOAA, as of July 2024, there have been fifteen confirmed weather or climate disaster events in the United States, with losses **exceeding $1 billion each.**

These “established” data loss threats are by now known and understood. And no, they aren’t going away.

What was surprising, then, was what we heard regarding our follow-up question. Can this level of confidence be explained by their adoption of best practices around the 3-2-1-1 backup strategy?

As it turns out, nearly one in four organizations may be overconfident on this!

**23%**
**of survey respondents say their organization hasn’t adopted the 3-2-1-1 backup strategy, and another 6% aren’t sure.**

# Ransomware: Broad Impact and Lasting Consequences

## Did You Know?

**The last "1" in 3-2-1-1 stands for immutable backup storage, vital to your disaster recovery and data loss prevention efforts. Immutable backups are saved in a write-once-read-many (WORM) format that unauthorized users can't alter or delete, so they provide a last-line defense against data loss.**

With a developing threat environment and the growth of ransomware services (RaaS), falling victim to a ransomware attack is a matter of when not if.

We’ve heard IT leaders say they feel ready and prepared. In practice, not all data gets recovered after an attack.

**80%**
**of surveyed organizations have been hit by ransomware.**

**30%**
**30% is the average percentage of data survey respondents couldn’t recover after being hit by a successful ransomware attack.**

And the recovery process remains time-consuming and disruptive to the business.

We've seen that most organizations can't afford to take more than 48 hours to recover from a data incident and maintain any hope of avoiding revenue impact.

**82%**
**of survey responders affected by ransomware claim that they recovered within 48 hours, while 18% did not.**

Natural disasters, insider threats, and ransomware are now ever-present. What's changed for these risk factors is that their probability of occurrence has increased, and so has their impact if (when) they materialize.

Preparation is the best defense. A robust data resilience infrastructure that consolidates your protection, backup, and recovery components into a unified data protection environment, implemented as part of a 3-2-1-1 backup strategy, should be your goal.

## SaaS Applications: An Underrated Pillar of Data Resilience

SaaS applications play a crucial role in almost every organization today.

Roughly 82% of responders indicated that their organizations use ten or more SaaS applications, highlighting the scale and their importance in the modern enterprise. These applications generate and use a lot of data, vital for keeping operations running smoothly and customers happy.

Many organizations have a blind spot when it comes to data within those applications:

Only a fraction of SaaS applications is monitored and secured by the organizations themselves.

**59%**
**of respondents' organizations use 10 to 30 SaaS applications**

**19%**
**use between 30 and 50**

**30%**
**of SaaS applications are not monitored / secured**

**Among the 70% that are monitored/secured, for 40%, that responsibility is outsourced/ unattended**

SaaS data is typically subject to the shared responsibility model, where the data owner (i.e. your organization) is responsible for data protection and data recovery.

**Example: Microsoft Shared Responsibility Model**

| | Customer | Microsoft |
|---|---|---|
| **Preparation** | • Business continuity and dissaster planning<br>• Documentation of known good states<br>• Monitoring and data retention<br>• Operational security | • Identity and access management functionality<br>• Tools for documentation<br>• Log availabillity and consistency<br>• Platform security |
| **Recovery** | • Restoring soft-deleted resources<br>• Restoring prior configurations | • Availabillity of soft-deleted resources (time-limited)<br>• Availabillity of APIs |

And yet, among the 40% of our survey respondents who said that their company had experienced data loss due to a SaaS application breach in the past year, just over half (51%) consider their SaaS provider to be at fault.

With this additional context, the importance of SaaS backup solutions becomes evident, as they deliver a high degree of security and autonomy for organizations that want to preserve their SaaS data without relying on the SaaS application vendors themselves.

## The Impact of Non-Compliance

Compliance requirements have been around for decades and are only strengthening. In parallel, enabling compliance is increasingly challenging, as IT infrastructure becomes more and more complex.

For example, the recent NIS2 Directive from the EU introduced more industry coverage and regulatory requirements.
There are developing regulatory frameworks worldwide that might have a similar impact in the future.

Almost half of responders confirmed that their organizations have dealt with regulatory fines brought on by inadequate data protection measures.

**NIS2 Directive, Article 21, Paragraph 2:**
**The measures … shall be based on an all-hazards approach that aims to protect network an information systems and the physical environment of those systems from incidents, and shall include at least the following:**

**Section (c): Business continuity, such as backup management and disaster recovery, and crisis management[5]**

**43% of respondents' companies faced regulatory fines due to inadequate data protection measures.**

Ensuring your company complies with relevant regulations such as GDPR, CCPA, and HIPAA isn't just vital to its reputation. Failure to do so can be costly.

What is the best way to stay compliant? The hard way is to have your internal teams seek consultation and guidance through third parties. The easier way is to employ a data resilience solution with built-in compliance levers, like access controls and versioning.

5 DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

## Summary

Even as organizations improve their data protection practices and data resilience posture, the risk of data loss and the importance of assuring business continuity remain top-of-mind topics for IT leaders. At the same time, there are visible discrepancies between expectations and reality, as organizations profess their dedication to data protection yet continue to suffer the conse quences of data loss.

And it's not a surprise. With ransomware and other potential threats, new risks emerge to businesses small and large (and in-between). Across the board, IT leaders seek additional investments in data protection, backup, and disaster recovery. Follow ing best practices in the field can help maximize protection under the constraint of limited budgets.

As the pioneer in Data Resilience, Arcserve is well-positioned to help. Arcserve Unified Data Protection (UDP) and Arcserve SaaS Backup are cost-effective data resilience solutions that are easy to deploy and quick to deliver value by ensuring recovery and minimizing downtime and data loss.

Arcserve is here to answer your questions and show you how to better protect your data wherever it resides. To learn more, contact us at arcserve.com/contact-us
Explore all Arcserve capabilities at arcserve.com/products-overview
Reach out to us at info@arcserve.com

## METHODOLOGY

Arcserve wanted to better understand how data security leaders get back to business in the event of a data breach or outage. Arcserve commissioned an independent research firm to survey 150 data security leaders in the US on data recovery and resilience. The audience is split evenly between SMBs (< 1000 employees) and larger enterprises (between 1000 and 5000 employees). The margin of error for this study is +/- 6.9% at the 95% confidence level.

**To see Arcserve data resilience solutions in action, request a demo at arcserve.com/request-demo**

## About Arcserve

Arcserve, a global top 5 data protection vendor and unified data resilience platform provider, offers the broadest set of best-in-class solutions to manage, protect, and recover all data workloads, from SMB to enterprise and regardless of location or complexity. Arcserve solutions eliminate complexity while bringing best-in-class, cost-effective, agile, and massively scalable data protection and certainty across all data environments. This includes on-prem, off-prem (including DRaaS, BaaS, and Cloud-to-Cloud), hyper-converged, and edge infrastructures. The company's four decades of award-winning IP, plus a continuous focus on innovation, means that partners and customers, including MSPs, VARs, LARs, and end-users, are assured of the fastest route to next-generation data workloads and infrastructures.