arcserve®

WHITE PAPER

Disaster Avoidance: Prevailing Against Data Threats and Financial Loss

Evolving beyond recovery to avoiding disasters altogether

Introduction

When companies experience losses of $1 million to billions whenever data loss events occur, executive teams pay attention. Multiply this number by the high likelihood of these events occurring five or more times each month, or 60 times in a year, and it's no wonder that investments in data protection are on the rise. The economic impact of data loss on productivity and the growing global threats to data sources cannot be denied, and it has a high price.

IT leaders across midmarket and decentralized enterprises are seeing these global trends and seeking the agility of today's cloud and hybrid solutions to mitigate this risk. But apart from finding new solutions or attempting to retrofit the ones they already have, their leadership is looking to go beyond backup; challenging their teams to seek out new methods that can, perhaps, enable them to avoid a disaster altogether.

In the wake of high-profile malware attacks that are seemingly paralyzing companies, large and small, around the world, many businesses are realizing that it's not enough to recover quickly; the real challenge is recovering *current* data. And while restoring systems and applications in sub 15-minutes is a great first step, you have to ask yourself:

> what is the point of recovery if what you're recovering is from yesterday?

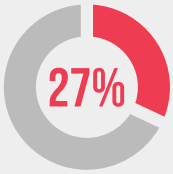
The Financial Woes of Data Loss

Data is a company's most valuable, and most vulnerable, asset. Used by every individual, it's at the core of a company's decision-making and productivity, not to mention its customer service and reputation. Just as a company wouldn't put its inventory or locations in a high-risk environment or leave it unguarded, so must today's corporations increase their vigilance to mitigate the risk of ransomware attacks, human error, data breaches and more.

Recent studies have found that companies are losing millions, if not billions, of dollars when data loss occurs. In the aftermath of a ransomware attack, system failure or human error event, companies need to consider restoration costs, as well as legal and communication fees, compliance fees, lost customer business, and increasing customer loyalty spend.

THE DIRECT COSTS.

The economics of a data loss demonstrate the financial impact of a simple outage. **A recent IHS study found that the cost of a single downtime event ranges from $1 million for midsize companies to more than $60 million for large enterprises, with a likelihood of five downtime events each month, on average.** The annual cost quickly reaches $60 million to $3.6 billion per company, or $700 billion to North America enterprises.[1]

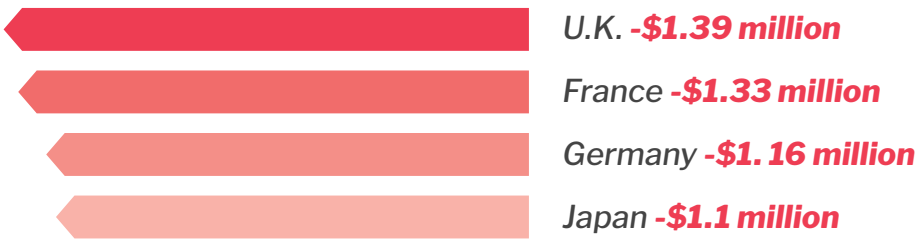


In 2017, Ponemon Institute's global study of the cost of data breaches reported the average cost of a lost or stolen record was $141 and each company has a 27.7% likelihood of a recurring material data breach in the next 24 months.[2]

THE INDIRECT COSTS.

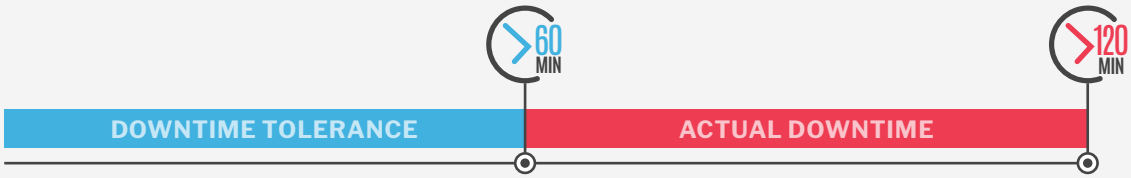
It's important not to ignore the long-term effects of a breach or data loss on an organization's customers and prospects. Ponemon Institute also reported that after a breach, **U.S. companies lost an average of $4.13 million** due to customer turnover, increased customer acquisition programs and diminished goodwill.

Globally, the impact was also significant with companies losing millions[2]



The impact on a company's reputation and bottom line are enough to make data protection not just an IT issue, but one that is discussed in corporate boardrooms. Not only is the risk and likelihood of data loss high, the tolerance for downtime when an incident occurs is decreasing.

According to IT analyst firm ESG, more than half of midsize and enterprise organizations have a downtime tolerance of less than one hour for high priority applications, and two-thirds of production systems have intended recovery times of two hours or less.



The difference between desired service level agreements (SLAs) and what can be realistically delivered tells a very clear story: backup alone isn't enough to ensure business continuity.[3]

The New Era: Disaster Avoidance

Data protection has become a core business requirement for companies of all sizes, regardless of location or industry. And just because a company may be small doesn't mean its employees and customers have a different tolerance for downtime or data loss; they simply demand uninterrupted access and protection. The requirements for data protection are fundamentally the same for all companies, regardless of size, location or industry.

However, for many midsize and decentralized organizations, employee and customer expectations often do not align with what IT teams can realistically deliver. In most cases, IT is asked to do much more with the same budget and staffing as before, while users are demanding 100% uptime to do their job, and more importantly, require corporate systems to safely guard their work by the minute. The discrepancy between "expectation versus reality" isn't sustainable, and underscores the need to evolve from simply backing up data in the event of disaster, to **avoiding the data loss disaster altogether.**
Unlike a specific software or hardware solution, the term "disaster avoidance" is the strategy and techniques used to minimize the effect of downtime, whereby infrastructures are built to withstand disasters and the subsequent damage often incurred. And while many organizations have data protection plans in place to combat the threat of data loss, most wouldn't be able to maintain availability in the wake of disruption.

That said, achieving 'always on' availability is often fraught with exorbitant costs, unnecessary complexity or the realization that 'availability' is, in most cases, access to day-old data which doesn't do anyone any good. It's this realization that drives most IT leaders to either throw up the white flag or overspend on complex solutions that may or may not meet their SLAs for unique systems and applications.

> data “availability” means access to day-old data, which doesn’t do anyone any good.

But getting to the place where you can run “business as usual” is dependent on taking steps now to avoid the disaster; whether it’s in the form of a data disaster, financial disaster or loss of customers.

Putting Disaster Avoidance Into Perspective

Imagine this scenario: a ransomware event causes your business to lose access to its critical email, CRM and financial systems. But without fear, you busily deploy the recovery plans you have in place, knowing you can get back online in ten minutes or less. And you’re right, you can, which should be great news, except for the fact that the last backup was run overnight, so all the data you’re recovering is from yesterday. The recovery time objective (RTO) was excellent, but the recovery point objective (RPO) caused the business to lose 12+ hours of critical customer and financial data.

Now imagine a different ransomware event causes your business to lose access to its critical email, CRM and financial systems; but, this time your RTOs and RPOs are in sync so now, not only can you get back online quickly, but you’ve avoided the disaster by restoring current data. Your data is now truly “available” and business runs normally.

You’re probably shaking your head, thinking, “easier said than done,” but it is attainable – and with much less complexity and cost than you may think.

Five Steps to Getting There

To move from managing backups to disaster readiness, IT administrators must take actionable steps now to prepare for the next data disaster. To do so effectively requires a proven methodology to assess, plan and execute the strategies needed to ensure your company is ready and working in tandem with technologies that can meet your strategic requirements.

1. **Create your risk profile:**

   Operational resilience is 110% tied to known business exposure and risk. Only organizations that know their risk profile can avoid disasters. Those that don’t know their risk profile can, and should, expect data loss and the subsequent consequences.

   Given this, you need to estimate your actual cost of downtime, keeping in mind that cost isn’t necessarily based on size of the organization; define and assign values as accurately as possible.

2. Understand your SLAs:

Seems like a no-brainer, but you can't fix or optimize what you can't measure. Look at the worst-case scenario – the worst case of known risk – to give business leaders the facts so they can make more informed decisions. Then, agree to service levels based on impact to the business: be clear on the true criticality of your workloads and data sets.

Classify your systems/data into tiers and define which systems you could go a few hours without, and those that are core to the business and your customers. Those are the ones you need to focus on when preparing to avoid disasters.

3. Pay special attention to your RPOs:

This step is likely one of the most important, but often one of the most overlooked. As we've pointed out, quick recovery times are great, but day-old data isn't helpful from the most critical systems and applications.

Avoid a data (and financial) disaster by getting your RPOs in sync with business requirements. **When considering solutions that guarantee availability with 15-minute recovery times, be sure to fully understand the RPOs that can be achieved. Is it possible to get also get 15-minute recovery points, and if so, how complex and costly is it?**

4. Focus on automation and follow the workload:

Take the manual aspects away to mitigate risks which leave you more exposed for data loss. There are a wide range of tools/technologies and infrastructures available to support your specific tolerance for downtime, and each one will bring you different levels of automation. The trick (and challenge) is applying automation across the entire ecosystem; all aspects of your data protection strategy need to be integrated.

You can't create an effective disaster avoidance platform with bolted-on solutions or those with very little coordination.

5. Consider new disaster recovery technologies:

Disaster recovery (DR) is commonly thought of as a "nice to have," and while most IT teams recognize the importance of having a DR plan in place, many haven't implemented one or don't consistently test it. For a wide variety of reasons ranging from expense and lack of resources, to fear of business interruption, many organizations shy away from deploying DR technology that could enable them to avoid disaster.

New cloud-first disaster recovery as a service (DRaaS) technology is changing the game, delivering RTOs and RPOs of minutes while being non-disruptive, easily-deployable and affordable. By leveraging DRaaS technology that offers near-zero data loss, one might ask, ***"if you recover fast enough, did the disaster even happen?"***

New DRaaS technology is changing the game, delivering RTOs and RPOs of minutes while being non-disruptive, easily-deployable and affordable.

Making Disaster Avoidance Practical

The conversation around disaster mitigation from an IT perspective can be boiled down to a simple but painful reality: mission-critical applications and data can't be down for long, if at all. Easier said than done if you're not using the right solutions.

Different from today's data protection, disaster avoidance promises not just data recovery, but data relevance. IT departments know how to quickly recover their systems to keep businesses operating, but the calls will quickly come in when users realize the data restored was hours (or days) old. Disaster avoidance is more than backup, it's ensuring that the data is timely and data loss is measured in seconds or minutes, not hours or days.

If you can easily or even automatically bring up an image of the systems and a copy of the data set that has been replicated at short intervals, you've essentially avoided the IT disaster that would normally ensue - and its dire financial consequences.

But finding technology to help you avoid disasters can be a cumbersome challenge as today's solutions typically fit into three categories:

1

HIGHLY COMPLEX

Highly complex and expensive; those that may be defined as "service bureau" solutions

2

ASSEMBLY REQUIRED

Those that offer high availability / continuous replication, but aren't easily deployable and therefore can be coined as "assembly required"

3

INEFFICIENT REPLICATION

Those that are self-service but lack highly-efficient replication, thus limiting users to recovering (at best) hours-old data, which simply doesn't cut it for the most critical applications

Ultimately midsize and decentralized enterprise organizations need something different to make disaster avoidance a reality, they require a solution that offers:

EASE OF USE:

Assembling a technology kit is not realistic, making an "out-of-the-box" or "ready to use" solution a requirement for most IT teams

SELF-SERVICE ACCESS:

Users need visibility, access and flexibility that can be managed through one portal, especially as the alternative is a costly service bureau

ORCHESTRATION:

Users must be able to initiate recovery using a sequence of predetermined events in the cloud, using failback if available

NEAR-ZERO DATA LOSS:

Businesses need more than quick recovery, they need recovery of current critical data, systems and applications to meet stringent RPOs

CROSS-PLATFORM SUPPORT:

IT teams need technology that comprehensively supports all midmarket platforms, hypervisors, cloud and on-premise systems to fully integrate all aspects of their DR strategy

FAILBACK:

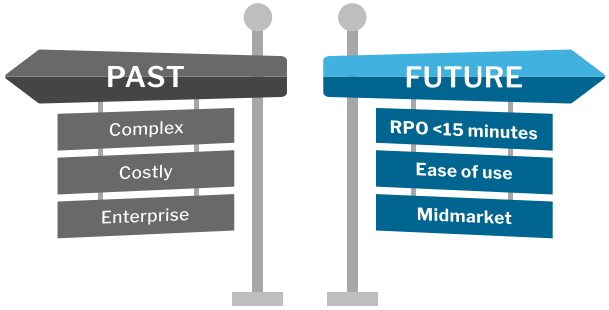
Having a disaster avoidance plan is one thing, but doing it is another. Users must be able to fully restore systems to their previous state after a failed system has been recovered in the cloud

AFFORDABILITY:

Most companies simply cannot afford highly complex solutions, making disaster avoidance unattainable. They need to mitigate spikes in costs through subscription pricing that aligns with cost-conscious budgets

A New Mindset

Given rising expectations and new data loss threats, backup operations are becoming disaster recovery strategies and, in the next 12 months, will become disaster avoidance platforms. This is the mandate from corporate boardrooms to their IT departments, regardless of company size or number of locations; the economic impact is simply too high.



The first step to achieving disaster avoidance is a new mindset. The data protection industry has traditionally focused on recovering data quickly, often measured in RTOs. The result is many companies are now able to restore their systems within minutes, which is a start, but users expect more. These companies need to shift their focus to the more difficult dilemma: the point of time in which their data was backed up. Ranging from hours to days for most midsize businesses, this will continue to evolve as cloud-first technologies fuel the next phase of data protection.

Taking the Next Step with Arcserve UDP Cloud Direct

Trusted by IT departments for their ERP, CRM and other core business systems, it's not surprising that direct-to-cloud data protection is experiencing rapid growth. According to Gartner, the number of enterprises using cloud as a backup target will double by 2020[4]. And it makes sense; the cloud provides the flexibility and agility that today's midsize and distributed enterprises require to achieve disaster avoidance.

Arcserve's direct-to-cloud DRaaS and BaaS solutions deliver what midsize and decentralized enterprise companies expect: near-zero data loss wrapped into a ready-to-use, easily deployable solution that can be up and running in minutes.

With UDP Cloud Direct, you receive:

RISK MITIGATION FOR BUSINESS-CRITICAL APPLICATIONS
Automated backups transfer data safely offsite with little-to-no need of regular human attention, while multiple validation points ensure data is fully recoverable

ANYWHERE, ANYTIME RECOVERY
The Arcserve Portal allows IT staff to manage users and reports, and back up, restore and recover applications and systems to and from anywhere with an Internet connection

HASSLE-FREE MANAGEMENT
With no hardware to procure, install, deploy, maintain and manage, you eliminate an additional point of failure from your architecture

RELIABLE HIGH PERFORMANCE TECHNOLOGY WITH POSITIVE ROI
An end-to-end service from deployment to failback that serves as insurance for companies that cannot afford, or choose not to invest in a secondary site for disaster recovery. Compared to other large-scale cloud providers, costs are significantly lower as dedicated engineers aren't needed to manage the cloud

Conclusion

Disaster avoidance is the answer to a global data protection industry in crisis. Growing at more than twice the industry average, Arcserve provides an expansive worldwide channel and support network for midsize and distributed enterprises with the expertise, support and resources that IT teams need to fully safeguard their businesses from financial and data disasters.

> It's a new era in data protection; one that doesn't measure availability by how quickly data can be recovered, but by how old that data is.

Bottom line: Relevance of data is what matters, and will serve as the success metric by IT leaders and boardrooms alike.

Sources:

1 "2017 Cost of Data Breach Study." Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview, IBM, 19 June 2017, www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN.

2 Stanganelli, Joe. "The High Price Of IT Downtime." *Network Computing*, 29 Jan. 2016, www.networkcomputing.com/networking/high-price-it-downtime/856595126.

3 "ESG Research Report: The Evolving Business Continuity and Disaster Recovery Landscape." ESG Interactive Research, Enterprise Strategy Group, 19 Feb. 2016, research.esg-global.com/reportaction/BusinessContinuityDisasterRecoveryLandscapeFeb2016/Marketing.

4 Morency, John P, and Neha Kumar. "Survey Analysis: State of Disaster Recovery as a Service in 2016 - A Reference Customer Perspective." Technology Research, Gartner, Inc., 25 Oct. 2016, www.gartner.com/doc/3491518/survey-analysis-state-disaster-recovery.

For more information on Arcserve, **please visit** arcserve.com