WHITE PAPER

NEXT-GENERATION SOLUTIONS FOR DISASTER RECOVERY:

Protecting Organizations in the Face of Growing Adversity

BY

Vice President, Managed Services Sales
Rob Lerner, DataBank

Vice President of Cloud Operations
Autumn Salama, DataBank

For IT and business leaders of highly interconnected, data-driven business environments, a comprehensive disaster recovery plan is not a "would-be-nice-to-have" option. It's critical to mitigate risk and ensure business continuity.

Next-generation disaster recovery solutions, such as disaster recovery as a service (DRaaS), are now helping companies do much more than simply recover from unplanned downtime: they're protecting critical business operations and maximizing the company's chance of continued success.

> "93% of organizations have suffered a data-related business disruption in the last 12 months. Yet, only 29% of the surveyed IT and business leaders expressed complete confidence in their current disaster recovery technology to recover data."
>
> IDC Research, "The State of Ransomware and Disaster Preparedness: 2022"

DATABANK
Data Center Evolved™

Table of Contents

Executive Summary

Companies face so much risk today from a wide and growing number of threats: cyberattacks, power outages, natural disasters, or other types of situations that can lead to downtime and require rapid recovery. In turn, each of these threatens business continuity, which can lead to financial consequences, potential regulatory fines and penalties, and a damaged reputation in the market.

Next-generation disaster recovery as a service (DRaaS) solutions and services successfully limit the overall risk and exposure, giving companies peace of mind that they can successfully recover from any disruption – and keep their businesses running.

This white paper explores the critical need for more effective disaster recovery solutions in today's digital landscape. It provides an in-depth analysis of potential causes of downtime – threats such as cyberattacks, natural disasters, human error, and application outages – while highlighting the specific challenges organizations face with traditional disaster recovery efforts.

This white paper also introduces next-generation disaster recovery solutions delivered "as-a-service" by managed service providers and demonstrates how they can offer improved resilience and peace of mind. Finally, we take a closer look at DataBank's DRaaS solution and show how it can deliver IT and business continuity and minimize risk with cost-effective, easily executable disaster recovery capabilities.

Introduction: The Real Dangers of Not Having an Effective Disaster Recovery Plan

To understand the full impact of disaster-related downtime, consider a fictitious example of a large eCommerce company, whom we'll call Odyssey eCommerce. This company has enjoyed steady growth, both in revenue and market share, and gained a large, loyal customer base and a strong online presence. The future looks bright.

One day, a sophisticated cyberattack hit Odyssey eCommerce's website and database. Business operations immediately ceased, and the company also suffered a data breach, compromising millions of records of customers' most sensitive data, including personally identifiable information (PII) and credit card numbers. The attackers demanded a hefty ransom in exchange for not leaking the stolen data.

Odyssey eCommerce struggled to respond effectively, in part due to inadequate disaster recovery planning. While the company thought it had a disaster recovery solution in place, it turned out that servers were not backed up adequately. Without a way to recover a second set of data, and no way to use encrypted data rendered inaccessible by the cyberattackers, Odyssey eCommerce's operations continued to falter.

The company's website remained down for days, leaving the company unable to process new orders, provide updates on orders in process, or respond to customers' questions. As news of the data breach spread, once-loyal customers lost their confidence in the company's ability to protect their information. All of this led to a tarnished reputation, a sharp decline in sales, and a real concern about whether Odyssey could ever get back on track.

Despite its attempts to negotiate with the cyberattacker, Odyssey eCommerce was unable to recover its customer's data, which would subject it to possible regulatory fines and class-action lawsuits in the future. With mounting financial losses, a newly damaged reputation, and increasing legal liabilities, Odyssey eCommerce faced some difficult decisions, including the real possibility that it would have to shut down its operations – the potential downfall of a once-thriving business.

Although this is a fictional example, it was (and continues to be) a reality for a long list of organizations, including Colonial Pipeline, Microsoft Exchange Server, CNA Insurance, Florida's Water Supply, and JBS. The threat underscores the importance of disaster recovery planning, including disaster recovery solutions and services, for any business looking to ensure business continuity.

REAL-WORLD STATISTICS, REAL BUSINESS CONCERNS

The average duration of downtime after a ransomware attack in the United States is nearly three weeks.[1]

For more than 90% of mid-sized and large enterprises, the cost of downtime exceeds $300,000 an hour.[2]

93% of companies without disaster recovery who suffer a major data disaster are out of business within one year.[3]

Nearly 95% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster.[4]

96% of businesses with a disaster recovery solution in place fully recover operations.[5]

The Causes of Downtime and Business Disruption

Today, availability has become the most valuable commodity for businesses of every size; yet, high-profile outages are now occurring at an alarming rate – threatening business continuity and even each company's long-term viability. Recent research shows that from 2019 to 2022, 96% of organizations experienced at least one incidence of downtime.[6] Organizations would be wise to consider any disruption to their operations to be a "when" event, not an "if."

With this mindset, organizations of all types need an executable resiliency solution because, beyond true natural disasters, they are vulnerable to a growing number of threats and risks, including cyberattacks (particularly ransomware), human errors, hardware failures, and many other events, both planned and unplanned.

1 Statista, "Average duration of downtime after a ransomware attack from 1st quarter 2020 to 4th quarter 2021," July 21, 2023.

2 Information Technology Intelligence Consulting, "ITIC 2021 Global Server Hardware, Server OS Reliability Survey Results," November 30, 2021.

3 Continuity Central, "Business Continuity Statistics: Where Myth Meets Fact."

4 Gartner, "Gartner Research and Advice for Disaster Recovery," September 1, 2017.

5 Continuity Central, "Business Continuity Statistics: Where Myth Meets Fact."

6 LogicMonitor, "IT Outage Impact Study: A Global Analysis of IT Downtime and its Impact on Business," 2023.

NATURAL DISASTERS

Natural disasters can be devastating and can severely restrict a company's ability to conduct business as usual during periods of extended downtime. Floods, fires, hurricanes, and record-breaking high and low temperatures can cause structural damage to a company's buildings and infrastructure and off-premises data centers. These events can cause power outages, overheating, hardware failure, and other consequences, making it difficult to maintain normal business operations or quickly recover from downtime and lost data.

Unfortunately, the threat of natural disasters will only increase in a future of climate uncertainty. Over the past five years, the United States has experienced an average of 18 climate disasters with damage over $1 billion – a significant jump over the 7.7 the country averaged for the four previous decades.[7] Experts predict the number and cost of weather and climate disasters will continue to climb in the future.

CYBER THREATS AND ATTACKS

Cyberattacks are an ever-present threat to any company's cybersecurity defenses, business operations, and data. Ransomware, in particular, is especially concerning: It now accounts for 20% of all cybercrimes and has become a nearly billion-dollar business for cybercriminals.[8]

According to additional research from the Verizon Data Breach Investigation Report, the median cost of ransomware has more than doubled in the past two years and the total number of ransomware attacks was higher in the last two years than in the past five years combined.

When successful, ransomware attacks can be devastating and can even bring vital operations to a halt. Colonial Pipeline suffered a ransomware attack in 2021 and was forced to pay a $4.4 million ransom and lost over 100 gigabytes of data. The attack lasted six days, leading to consumer panic and an increase in gas prices in locally affected areas. If these events weren't bad enough, Colonial Pipeline was later fined nearly $1 million for non-compliance and "failure to adequately plan and prepare for manual shutdown and restart of its pipeline system."[9]

HUMAN ERROR

Where natural disasters and high-profile cyberattacks tend to garner the most attention, human error is actually the leading cause of downtime. According to the most recent Verizon Data Breach Investigations Report, "the human element was involved in approximately three-quarters (74%) of the analyzed breaches."[10]

Examples of human error can include falling prey to social engineering, phishing, or business email compromise (BEC) campaigns, lost or stolen credentials, or even just a wrong keystroke in an important line of code.

In 2017, significant portions of the internet were crippled when Amazon's Simple Storage Service cloud experienced an outage. The culprit? An employee's typo that accidentally took a large number of servers offline – resulting in a cost of $150 million to S&P 500 companies and U.S. financial service companies and $160 million in lost revenue for U.S. financial service companies.[11]

---

7 Forbes Advisor, "Natural Disaster Facts and Statistics 2023," June 7, 2023.

8 AAG, "The Latest 2023 Ransomware Statistics," August 2, 2023.

9 Industrial Cybersecurity Pulse, "Colonial Pipeline fined almost $1 million," July 8, 2022.

10 Verizon, "2023 Data Breach Investigations Report."

11 Vanity Fair, "One Amazon Employee's 'Human Error' May Have Cost the Economy Millions," March 3, 2017.

HARDWARE FAILURE

Hardware failures are another common cause of downtime. In 2022, 24% of organizations experienced server downtime due to outdated hardware.[12] Unfortunately, when hardware fails, it may be a long time before the problem can be fixed since it may be difficult to identify and troubleshoot the issue, reboot or service the hardware in question, or possibly even replace it.

Hardware failures can often be prevented by proactive maintenance, but if companies don't have adequate IT resources or sufficient time, maintenance may be a luxury they simply can't afford.

POWER OUTAGES

Unfortunately, it doesn't take a Category 5 hurricane to cause disruptions and downtime. It may be as simple as a common power outage. One survey found that power outages alone cause nearly 35% of unexpected downtime.[13] In addition to downtime, power outages can also result in data loss and even the corruption of data storage.

COOLING ISSUES

Server rooms and data centers generate significant heat, emphasizing the need for cooling systems capable of preventing equipment from overheating or experiencing other damage. Without effective backup cooling systems, server racks could overheat and lead to downtime, especially if not enough cold air is distributed to the network and computing equipment. At high temperatures, equipment can be damaged and/or shut down to protect itself.

No matter the cause, any downtime is unacceptable and subjects the company to too much business risk. Worse, many companies may think they have adequate systems and controls in place now, only to learn their existing disaster recovery solution presents real gaps related to data backup and restoration.

FAILURE IS NOT AN OPTION: THE CONSEQUENCES OF DOWNTIME

- Lost revenues
- Loss of customer trust
- Reputational damage
- Missed business opportunities
- Surprisingly high costs related to recovery
- Potential fines, penalties, and lawsuits

12 Information Technology Intelligence Consulting, "Security, Data Breaches Top Cause of Downtime in 2022," April 8, 2022.
13 Invenio IT, "7 Strategies to Avoid Data Loss from Natural Disaster," October 11, 2022.

Challenges Posed by Traditional Recovery Methods

Many organizations believe they have an effective disaster recovery solution as a cornerstone in their overall cybersecurity defenses. Yet chances are good that they still face significant limitations and challenges when it comes to ownership, daily use, and efficacy.

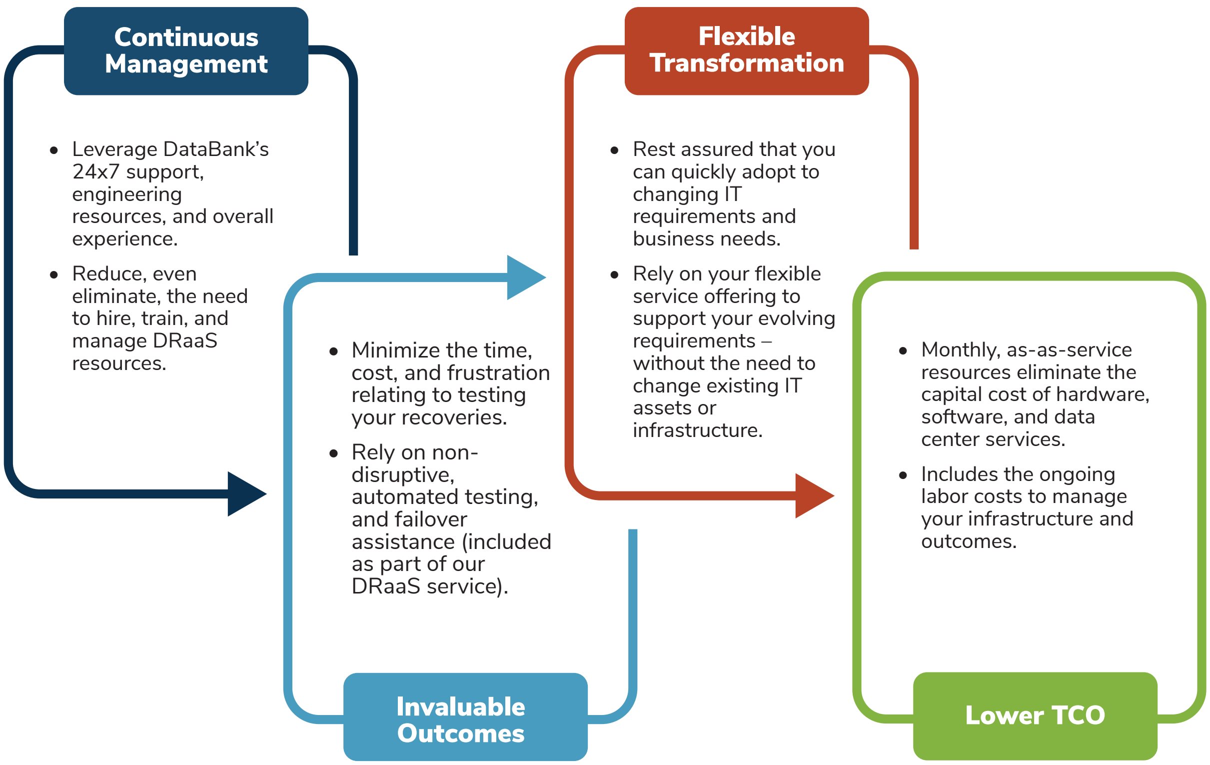
- **High cost of ownership:** Many disaster recovery solutions are expensive to purchase, implement, manage, and maintain. They can also be time-consuming to operate, requiring extensive hands-on involvement from IT and preventing valuable team members from focusing on higher-value work initiatives.
- **The need for specialized skills:** Similar to the point above, IT and business users may need specialized skills, extensive experience, or the ability to come up with creative workarounds to make legacy disaster recovery solutions support the company's "this is how we've always done things" approach.
- **Lack of scalability:** Many outdated disaster recovery solutions simply can't scale to keep pace with the company's growth or changing requirements. As a result, the company may be operating in the dark when it comes to the type and volume of data it believes it's backing up – leading to the potential for unpleasant surprises down the road.
- **Backup data access related to recovery point objective (RPO):** RPO describes the interval of time that may pass during a disruption before the quantity of data loss during that period exceeds the company's tolerance level. If the company can't access a good copy of backup data within the parameters of the planned RPO, the company may suffer a serious and irreparable disruption.
- **Lengthy recovery time objectives (RTO):** RTO is the amount of time after a disaster that a business has to restore business processes to an acceptable service level to avoid unacceptable consequences. Similarly, without an effective data backup and restoration component as part of its legacy disaster recovery solution, a company may suffer lengthy RTO times that exceed its goals.
- **Missing or limited communications plans:** Comprehensive, well-communicated disaster recovery plans are needed to keep employees informed and the business running as effectively as possible during outages and downtime. Many companies overlook this important component of their overall business continuity plan (BCP), subjecting themselves to additional risk when it comes to surviving a cyberattack or a natural disaster.
- **Additional cybersecurity and compliance risks:** Continuing to rely on ineffective legacy disaster recovery technology can present additional cybersecurity risks and ongoing uncertainty. Furthermore, many companies may find it difficult to comply with stringent data privacy regulations, which could subject them to fines, penalties, and reputation damage.

These challenges and limitations signal that the time is right for companies to move beyond old ways of thinking about disaster recovery and begin to consider next-generation innovations and managed services approaches that are already proving to be more effective at protecting them from any adverse event.

Why "as-a-service?"

As the acronym implies, DRaaS is a service, not a product. While your solution will surely involve industry-leading hardware and software platforms, the keys to successful outcomes center around the experience, expertise, and service components of your provider.

In order to help you achieve your RTO and RPO objectives now, and for years to come, it is advisable to seek partners and service-based solutions, so you don't have to worry about internal staffing or re-evaluating the underlying hardware and software platforms as your needs change.



Designing for Failure: Why Do We Need to Plan for Potential Outages?

It is important to emphasize that even the most redundant systems can't offer 100% protection. Each system represents a single point of failure in the overall architecture. If an entire system goes down, it could trigger a chain of events that threaten business continuity and can't be overcome, even with multiple redundancies. For example, a redundant storage system with highly available controllers and other elements could still completely fail due to a software bug. This makes it critical to have a disaster recovery solution, even for the most highly available applications and systems.

In addition, companies need proactive risk management strategies and technology that will complement existing solutions such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), DDoS mitigation solutions, and other cybersecurity tools to develop a comprehensive way to prevent, detect, and respond to cyber threats and potential downtime.

This is crucial in minimizing downtime and ensuring business continuity. Disaster recovery helps companies restore data and resume operations in the shortest time possible after disaster strikes. Disaster recovery solutions encompass comprehensive backup strategies, redundant systems, and failover mechanisms that allow for a seamless transition to backup systems in the event of system failures, cyberattacks, or natural disasters.

By minimizing downtime and data loss, disaster recovery solutions enable businesses to continue serving customers, managing operations, and maintaining productivity even during challenging circumstances. This continuity helps prevent revenue loss, preserves customer trust, and upholds the company's reputation as a reliable partner committed to data security, even in the face of adversity.

In addition to these benefits, disaster recovery delivers cost savings by minimizing the financial impact of downtime and other disruptions. This helps in the more obvious area of avoiding revenue loss, but as described above, disaster recovery helps maintain ongoing customer satisfaction and loyalty while reducing the need for expensive recovery measures. Using centralized management and automation, these solutions also optimize resource allocation, enabling efficient utilization of IT infrastructure and reducing operational overhead.

In the event of a data breach or loss, disaster recovery solutions enable rapid recovery, a critical step in helping companies meet regulatory obligations related to data restoration and reporting. The ability to maintain operational continuity during disruptions also showcases a proactive approach to risk management, aligning with compliance frameworks that emphasize the need for business resilience. As a result, disaster recovery not only safeguards sensitive information, but also enhances a company's ability to adhere to relevant compliance standards and regulations.

Next-Generation Disaster Recovery: The DataBank Difference

In today's interconnected, data-driven business environment, having a comprehensive disaster recovery plan is essential, despite previous shortcomings and limitations posed by traditional approaches. With the right strategy and provider, achieving the continuous availability of critical data, applications, and systems does not have to be an expensive, time-consuming process.

For example, with DataBank's disaster recovery service, there's no need for overburdened technical resources to set up and manage a duplicate production system in a secondary data center or attempt to rely on backups at an offsite location. DataBank owns all of the components of the disaster recovery platform and employs the engineering expertise, so implementation, migration, and support are all performed in house.

We offer one other important differentiator: our comprehensive process for helping you navigate from where you are to where you need to be. A wide range of organizations – of all types and sizes – already leverage disaster recovery experience, expertise, migration assistance, and personalized services to achieve the outcomes they need to protect their business.

THE DATABANK SOLUTION

DataBank's DRaaS solution gives companies an effective, easily executable disaster recovery service as a managed service offering. We manage the process to protect any organization's IT environment infrastructure to enable the business to quickly resume operations in the event of a disruption.

Our DRaaS solution offers the right combination of convenience with proven disaster recovery capabilities. Companies can still develop their own RTO and RPO thresholds, and we help them adhere to these parameters for a fraction of the cost. Our solution is backed by an expert engineering team, proven data protection methodologies and compliance, 24x7x365 support, and SLAs that meet, even exceed the toughest uptime requirements.

How Do You Know You Are Working With the Right Partner?

BASELINE: A REVIEW OF YOUR BUSINESS OBJECTIVES

- What data and applications are we trying to protect?
- What are we trying to protect ourselves from (cyberattacks, natural disasters)?
- Do our business stakeholders agree that these need to be protected?
- Have we prioritized your strategy with categories such as "life-critical," "mission-critical," "important," and other designations?
- Have we assigned recovery point objectives (RPO) and recovery time objectives (RTO) for each?
- Have we calculated the cost of downtime and business impact?
- Do we have applications or business processes that have specific compliance requirements?

A REVIEW OF TECHNICAL REQUIREMENTS

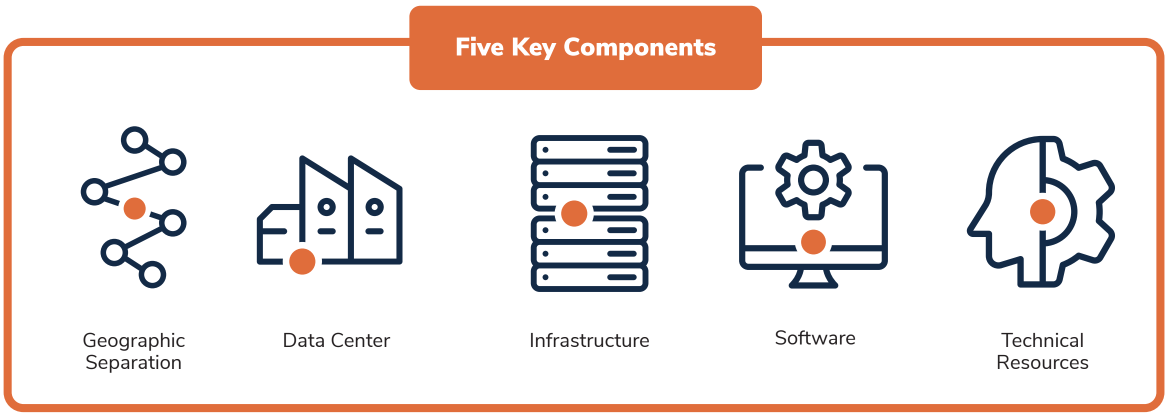
- Where do our data, applications, and systems currently reside geographically?
- Are we currently using a data center? If so, is ours reliable, accessible, compliant?
- How are we currently backing up/replicating our data today?
- What cybersecurity solutions do we use (IDS, IPS, DDoS, other)?
- What kind of networking environment are we using (dedicated, shared, fiber, MPLs, internet)?
- What type of storage environment(s) are we using?
- Have our retention policies been reviewed?

ADDITIONAL DISCUSSION

- How will the solution be implemented and/or migrated?
- What staffing and resources are needed to support the environment?
- Have we considered change management as our needs evolve?

The Five Key Components of a Comprehensive Disaster Recovery Solution

Solution providers can commonly provide the infrastructure resources (CPU, memory, disk) as well as the software to power your solution. Next-gen solutions are differentiated by also providing the data center(s), geographic separation, and the technical resources needed by a single provider who has control of the outcomes you need.



DataBank provides an executable, testable, and verifiable disaster recovery plan that meets the needs of your business and the demands of security, compliance, uptime, and recoverability.

Summary and Conclusion

Let's face it: Most organizations today already face more than their fair share of daily challenges as they seek to grow the business, outpace the competition, and increase market share. The last thing they need is unplanned downtime that completely disrupts vital operations and even threatens their future success.

Many business leaders operate from the mistaken belief that they are adequately prepared for disasters and/or downtime. Yet in many cases, they face unpleasant surprises – and hard decisions – when they learn that their rudimentary disaster recovery system failed when they needed it most.

Next-generation disaster recovery solutions – such as a modern DRaaS offering delivered by a capable managed service provider – are a proven way to overcome common limitations and subsequent business failures. Implementing such an approach can give any organization a better way to improve cybersecurity resilience, prevent downtime, and keep their business up and running at all times.

Next Steps

If you have questions about how to get started or how to develop a disaster recovery strategy for your organization, download the DataBank Disaster Recovery Planning Checklist.

Download Now

DATABANK

About DataBank

DataBank enables the world's largest enterprises, technology, and content providers to consistently deploy and manage their infrastructure, applications, and data on the right platform, at the right time, in the right place. Our colocation and edge infrastructure footprint consists of 65+ data centers and 20 interconnection hubs in 27+ markets, on-ramps to an ecosystem of cloud providers, and a modular edge data center platform with virtually unlimited reach.

We combine these platforms with contract portability, managed security, compliance enablement, hands-on support, and a guarantee of 100% uptime availability, to give our customers absolute confidence in their IT infrastructure and the power to create a limitless digital future for their business.

To learn more about DataBank, and how we're helping our customers achieve their goals related to disaster recovery, please visit www.databank.com or Contact Us today.