
# The Most Common Mistakes in Disaster Recovery and How to Avoid Them

# Table of Contents



# Chapter 1:
# Primary Objective

## Introduction

**Disaster recovery (DR) is essential for all organizations, regardless of size or industry. Natural disasters, cyber attacks, and hardware failures can cause significant disruptions to operations, leading to downtime, data loss and reputational and financial damage. DR plans help organizations recover more quickly from these events, minimizing the impact on operations and restoring critical data and systems as soon as possible.**

In addition to protecting operations, DR is critical for maintaining client confidence. Customers expect organizations to be available 24/7, and any downtime or data disruption can potentially lead to loss of business. DR plans help organizations maintain availability and credibility in the eyes of their customers, even during times of crisis.

Furthermore, many industries are subject to regulatory compliance requirements that include disaster recovery, HIPAA and FFIEC being two better-known examples. Failure to comply with industry regulations can lead to significant financial and legal penalties.

**This eBook will help you better understand why a comprehensive DR plan is critical for any successful organization while laying out common mistakes to avoid.**

**The average time to identify and contain a data breach is 287 DAYS.**

Ponemon Institute's Cost of a Data Breach Repors



# Chapter 2:
# Eight Common DR Mistakes

**Disaster recovery is a critical aspect of any risk management strategy. It involves having procedures in place for effectively responding to unexpected events that can disrupt normal operations and cause significant damage to a company's reputation, finances and employees. However, despite its importance, many companies still make missteps in DR planning and execution.**

## 1) Lack of a Disaster Recovery Plan

**One of the biggest mistakes companies make is not taking DR seriously and failing to allocate sufficient resources and attention to the process.**

Many businesses have a DR plan wholly inadequate for their needs or fail to have one. Organizations believe disasters are unlikely to happen or the impacts will be minor and therefore do not invest the time, money and effort required. However, such complacency is dangerous, as disasters can occur anytime and have far-reaching consequences for the unprepared.

Additionally, there often needs to be clarity about what constitutes a DR plan. Many assume that data backup and disaster recovery are interchangeable. While both are critical components of business continuity, it is essential to note that they are NOT the same.

**To read further about the differences, check out Data Backup vs. Disaster Recovery: Why Knowing the Difference Matters**

**The average cost of downtime is $88,000 PER HOUR OR $1,467 PER MINUTE.Veeam's 2022**

Data Protection Report

## 2) Failure to Adequately Identify RTO and RPO

**Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are crucial metrics in disaster recovery planning.**

RTO and RPO are essential in determining appropriate recovery approaches. Failing to identify these metrics can lead to a plan that inadequately prioritizes critical systems and data recovery or includes unnecessary processes and procedures.

Failure to accurately identify RTO and RPO ultimately results in misaligned recovery strategies unsuitable for the organization's specific needs. An organization may be unable to recover systems and data within the required timeframes, leading to significant disruptions and financial losses. Conversely, unnecessarily stringent RTO and RPO results in an organization over-investing resources in recovery capabilities leading to unnecessary expenses.

## 3) Insufficient Testing

**Test, test, test! Lack of testing leads to a false sense of security that a plan will work as intended.**

An organization can only validate effectiveness or identify improvement areas with proper testing. Testing can involve a live DR test, an isolated bubble test or a combination of the two.

Testing allows organizations to detect gaps, such as hardware or software compatibility issues, procedural inconsistencies or overlooked dependencies, and address them before a disaster occurs. Furthermore, testing provides an opportunity to train staff on DR procedures and ensure they can execute responsibilities correctly, minimizing downtime during an actual disruption.

# Chapter 2:
# Eight Common DR Mistakes Cont.

## 4) Outdated Plans and Procedures

**An out-of-date DR plan can be almost as harmful as having no plan.**

Organizations should regularly review DR plans and adjust them to remain current and effective. Technology and business processes continually advance, and outdated methods and procedures lead to ineffectiveness that falls short of meeting recovery objectives. Failure to evolve will result in obsolete methods, unsupported hardware or software and a lack of contingency planning for new business processes.

## 5) Communication Breakdowns

**In a disaster scenario, communication is imperative for ensuring all parties know the situation and follow established procedures—a lack of clear and effective communication results in delays, missteps and errors that compromise recovery.**

A DR plan should include detailed actions and contact information for all stakeholders involved in the recovery process. Internal teams, external vendors, customers and other relevant parties should all be considered when planning DR communications. Finally, it is essential to test the communication plan to ensure it is effective and to keep it updated to reflect staff or contact information changes.

## 6) Inadequate Security Measures

**Security is essential in protecting the organization's data and infrastructure before, during and after a disaster.**

Insufficient security measures result in unauthorized access to critical systems, theft of sensitive data or breaches that can impede recovery and cause additional damage.

Effective DR security measures should include access controls, backup and recovery procedures and encryption of sensitive data. Regular security testing and monitoring should also be conducted to identify and address potential weaknesses. Failure to implement appropriate security measures exposes an organization to unnecessary risk, resulting in prolonged downtime and costly damages

## 7) Lack of Training and Awareness Programs

**Without proper training, staff members may not understand their roles and responsibilities during a disaster, leading to confusion and delays in recovery.**

Moreover, staff members unaware of the DR plan may not be able to recognize potential risks and threats, leaving the organization exposed to additional vulnerabilities.

An effective, comprehensive training and awareness program should cover the DR plan's contents, processes, members' roles and responsibilities. Additionally, frequent training and awareness ensure staff is up-to-date on all changes.

## 8) Not Considering the Cloud

**Disaster Recovery as a Service (DRaaS) is cloud-based and provides comprehensive disaster recovery solutions.**

Providers offer various support options to organizations, including backup and recovery, replication, failover and testing, making

DRaaS an attractive option for organizations looking to improve DR capabilities.

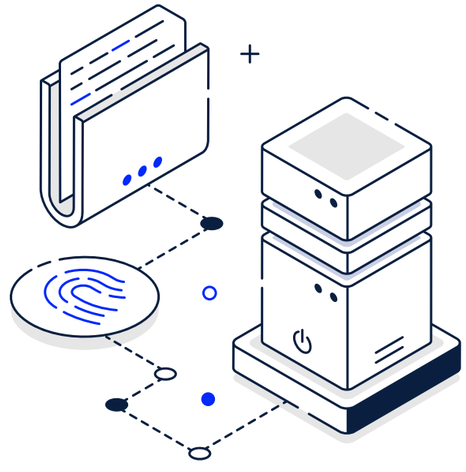
Organizations with limited IT resources or complex IT environments should particularly consider DRaaS. Cloud-based DR provides cost-effective, fast, reliable and scalable solutions, allowing companies to focus on core business activities while protecting critical data and applications.



# Chapter 3: Disaster Recovery as a Service (DRaaS)

**A complete DR plan is complex, consuming staff, time and money, and must be capable of evolving alongside the organization. DR is not a one-and-done event and requires continual maintenance and monitoring. Due to this resource-intensive nature, many organizations struggle internally to implement plans and procedures.**

**While traditional DR solutions have been around for years, businesses are increasingly turning to DRaaS as a preferred solution.**



## The Benefits of Data Recovery as a Service

**Cost-effective**
Traditional DR solutions require significant hardware, software, infrastructure, maintenance and support investment. DRaaS is subscription-based and eliminates the need for substantial upfront expenses. Organizations can choose the level of service they require and pay only for what they use without investing in additional infrastructure.

**Flexible**
Provides greater flexibility and agility versus traditional solutions. Providers offer recovery options, including on-premises, cloud and hybrid solutions. This variety means organizations can choose the recovery option that best suits their needs without being tied to specific locations or infrastructures.

**Highly Scalable**
A perfect fit for growing or shifting organizations. With traditional DR solutions, organizations must purchase additional infrastructure as needs evolve, which can be timeconsuming and expensive. Purchasing hardware for DR that sits idle, waiting for a potential DR event, is inefficient and costly. DRaaS allows organizations to quickly and easily scale up or down as needed.

**Support**
Ideal for companies lacking expertise or resources to manage traditional DR solutions. It provides a wide array of support, including testing, monitoring and management, helping organizations ensure their DR solution is up-to-date and functional. Businesses can be confident their data and applications are secure and available via robust security measures, including encryption, multifactor authentication and continuous monitoring.

# Chapter 4:
# OneNeck and ReliaCloud®

**OneNeck offers reliable, flexible, secure DR options tailored to an organization's needs. While we offer numerous hyper-scale cloud and on-premises DR options, backup and DR in ReliaCloud (built on Nutanix™) is often a perfect fit.**

OneNeck DRaaS on ReliaCloud protects critical applications and data from disruptions caused by natural disasters, human errors or cyber attacks. OneNeck delivers a comprehensive suite of DRaaS solutions, ensuring minimal downtime during a disruption. Robust SLAs and 24/7 support back our PCI, SOC 1, SOC 2, and HIPAA-compliant platforms.

Our experts understand DR readiness requires identifying business priorities, mapping application dependencies and fusing multiple solutions (provisioning a second site, setting up replication, defining a DR runbook, configuring
security policies and setting up networking connectivity). Each solution must be installed, configured and maintained separately, resulting in substantial initial commitment and continual operational responsibility.

**We help simplify the process by converging all these elements. ReliaCloud is purpose-built on Nutanix web-scale platform and offers all of the benefits of Nutanix Disaster Recovery with nearly instantaneous restore, ensuring your important data is secure.**

**93% OF WESTERN BUSINESSES experienced a disruption in the past year, and 68% HAD FOUR (4) OR MORE DISRUPTIONS.**

**International Data Corporation survey**



# Chapter 5:
# Need Further DR Assistance?

OneNeck's ReliaCloud Managed DRaaS will eliminate the complexities of managing a full-blown data center for DR.

**Initial Setup –**
OneNeck engineers set up the policy administration, configure systems, provide DR architectural blueprints, drive and compile requirements gathering to assist clients in deploying their chosen DR solution.

**Management –**
Our DR Coordinators oversee the plan and work to ensure all solutions are in place, maintained and verified. Coordinators schedule and lead exercises, act as a liaison for auditing and examining DR procedures, and through data gathering and extensive client interaction, develop updated runbooks.

**Testing –**
Let us tackle the burden of testing and validation. Our team will conduct all necessary DR testing laid out by the DR blueprint to ensure solutions are fully operational and up-to-date.

**Don't wait for disaster to strike. Contact a OneNeck DR expert today to find your right-fit backup and disaster recovery solution**

# Digital Infrastructure Solutions Built for Your Business

**US Signal, established in 2001, is a premier national digital infrastructure company that operates a fully owned fiber network to deliver a wide range of advanced digital solutions. Our offerings include robust cloud services, secure colocation facilities, high-performance connectivity, comprehensive hardware resale, and managed IT services, empowering businesses to enhance their operational efficiency through tailored network, data center, data protection, and cybersecurity solutions.**