Beyond Disaster Recovery

Why you need a different strategy when cyberattacks strike

READIVERSE

Commvault

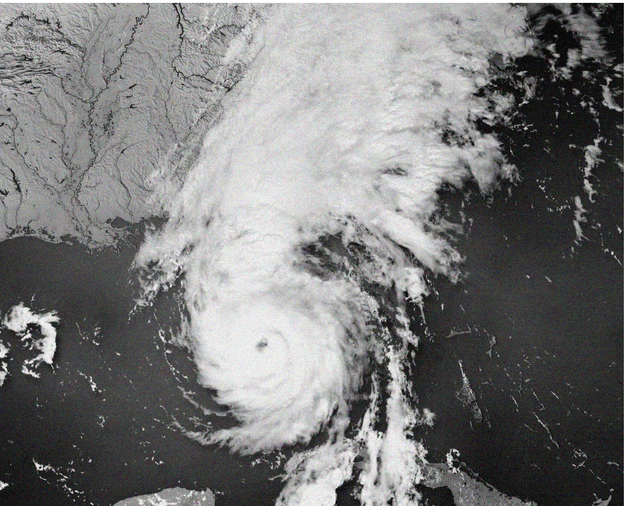
Your Approach to Recovery →Starts Here

From weather events to malicious cyberattacks, there's no shortage of destructive events threatening your business operations these days. Our newsfeeds are filled with the tales of harm from hurricanes to ransomware.

As part of any good business continuity practice, you need a plan for how your organization will bounce back quickly after an incident. You'll want to focus on protecting your employees, your customers, and all of your data, while mitigating the damage to your assets, finances, and reputation.

But remaining resilient in the face of these threats requires vigilance. Disaster recovery and cyber recovery are not one and the same, so it's critical to understand the differences. Read on to learn why you need to have both types of recovery planning in your arsenal – and learn how defining minimum viability at your organization is a key part of cyber recovery.

With thorough preparation, a comprehensive testing strategy conducted regularly, and solutions for fast recovery and rebuild of all your apps and data – you'll be empowered to overcome the challenges of recovery.



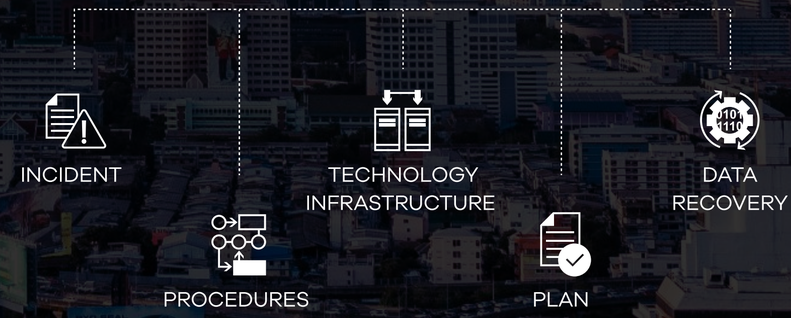
Why You Need

Disaster Recovery

You need a disaster recovery plan to handle predictable events like hardware failures or natural disasters like fires and floods.

In general, these incidents aren't intentional and do not actively target your data. Disaster recovery usually follows a pre-defined plan with established steps to restore systems quickly. Restoring from backups helps you get back online even if some data is lost. This process aims to maintain continuous business, minimize long-term impact, and protect critical data.

DISASTER RECOVERY PROCESS



Why You Need
Cyber Recovery

In contrast, cyber recovery tackles malicious attacks like ransomware or data breaches, where attackers actively try to harm your systems and corrupt your data.

This could be a subset of data or the entire infrastructure, including a disaster recovery failover site. Cyberattacks often involve investigation and remediation before recovery, which can extend the timeline.

You need to contain the attack and confirm no exploits remain. Every element of your environment, from hardware to data and backups, must be scrutinized for infection before restoring, as attackers might have hidden malware or altered backup files. You will need to minimize the damage, prevent data loss, and maintain security posture.

Get Back to Business with Minimum Viability

When a cyberattack knocks your organization offline, the pressure is on to restore operations as quickly as possible in order to minimize financial and reputational damage. So, one important aspect of cyber recovery is defining your company's minimum viability – that is, the minimum set of systems, data, and processes that you need to recover to remain operational after a disruption.

01 Identify critical assets
This includes **systems** (infrastructure, mission-critical apps, communication tools); **data** (operational, compliance, backup); and **processes** (business operations, IT and security, customer engagement).

02 Assess the impact of an outage
How much does it cost your organization when you aren't operational? Understanding the effects of downtime on each of your critical assets is vital to decision-making and helping prioritize their recovery.

03 Create a plan
Next, you need to create your plan to restore your most critical assets in the event of an outage – and test, test, test. Make sure your employees are trained on their role in recovery.

04 Focus on clean, validated recovery
It's important to note that you should validate you are recovering a clean copy of your data; having air-gapped copies will help enable faster recovery of that data. And you should conduct forensics in an isolated recovery room to find the root cause and help prevent future attacks.

Know the impact of an outage:

$4.88M

The average cost of a breach[1]

$14,056

The average cost of each minute of downtime[2]

24 DAYS

The average downtime after a ransomware attack[3]

[1] Cost of a Data Breach Report 2024, IBM
[2] IT outages: 2024 costs and containment, Enterprise Management Associates
[3] Statista

Cyber Recovery-Ready Design Scope

SCENARIOS

Cyber recovery generally drives a different set of needs vs. disaster recovery/business continuity plans.

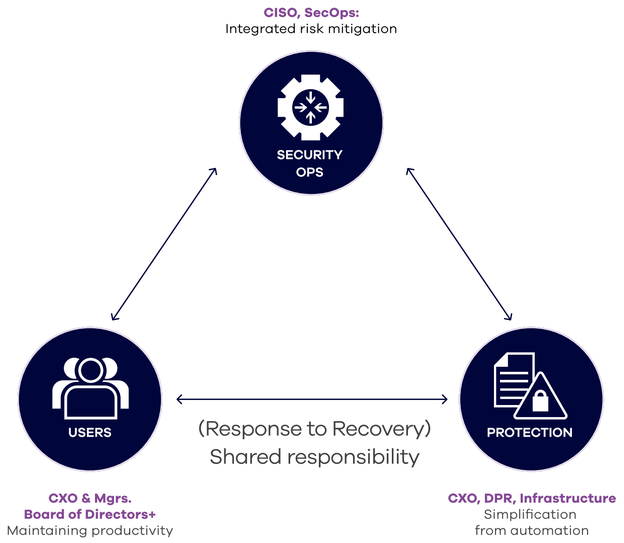
These strategies can be blended to converge resources and processes.

ELEMENTS	DISASTER RECOVERY / BUSINESS CONTINUITY	CYBER RECOVERY
COMPROMISE	Full-site loss of operations	Data, networks, security
RECOVERY	Failover/back RTO, rebuild	Selective restore to repair
RESOURCES	Full availability stack	Validation, restore, rebuild
PLANNING	Persistent	Elastic

ORGANIZATION

Cyber recovery involves collaborative shared responsibility outcomes across the organization (people, process).

Integrating and automating notifications, informed actions, and seamless workflows across the teams can accelerate the outcomes.



Cyber Recovery-Ready Design Scope

CAPABILITIES

Cyber recovery requirements depend on the goals of the organization.

- **Secure, isolated, and immutable vault backups**
- **Early detection of suspicious patterns**
- **Cyber analysis and data sanitization**
- **Automated recovery validation**
- **Planned, rapid recovery**

Disaster Recovery Testing Is Not Enough

Disaster recovery testing is important, but cyber recovery is much more comprehensive. While both aim to restore operational functionality after disruptions, fundamental differences necessitate distinct responses. Traditional disaster recovery plans struggle to effectively address the nuanced threats and complexities cyberattacks pose.

Therefore, while disaster recovery plans provide a valuable foundation for incident response, relying on them in the face of a cyberattack can be perilous.

A dedicated cyber recovery plan, backed by specialized tools, personnel, and frequent testing, is essential for mitigating these malicious attacks' specific risks and complexities.

HERE IS WHY:

- NATURE OF THE THREAT
- SCOPE AND FOCUS
- METHODS AND TOOLS
- DATA INTEGRITY AND VULNERABILITY

Cyber Recovery Testing is Critical

Cyber recovery testing is an actual practice run (or operational test) of restoring an application and its data from a backup. This is the kind of restoration process that will happen in a cyber incident, and it is the process that NIST recommends.1 Disaster recovery testing and cyber recovery testing each have their place for applicable scenarios, but cyber recovery is much more comprehensive.

Cyber recovery testing enables resilience for your systems and data, as well as business continuity. Recovering critical applications and data is fraught with complexity and issues. Testing cyber recovery helps uncover errors and resolve them when the stakes are low.

Testing will give your teams practice and confidence that they can recover critical applications and data when a cyber incident occurs.

In fact, NIST recommends “backups of data are conducted, protected, maintained and tested,” because “it is better to identify an unexpected issue during testing than during an actual cyber event.”1 But the reality is that very few organizations test fully, frequently and successfully.

CRITICAL NUMBERS

194 DAYS
is the average time an attacker is in an enterprise[2]

Attackers start moving laterally within

48 MINUTES
of an attack[3]

82% OF COMPANIES
that pay the ransom don’t get all of their data back[4]

1. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf
2. https://www.ibm.com/reports/data-breach
3. https://go.crowdstrike.com/2025-global-threat-report.html
4. https://www.hiscoxgroup.com/news/blog/hiscox-cyber-readiness-report-2024

How Commvault Helps

With Commvault, you can:

- Secure critical data with air-gapped copies
- Test frequently to confirm your plan works and employees know their roles
- Validate that you are recovering a clean copy of your data
- Conduct forensics in an isolated cleanroom recovery environment

COMMVAULT SOLUTIONS:

Commvault® Cloud for AD: Enterprise Edition

Identity and access management are vital to restoring your operations after an attack. This solution allows you to safeguard and accelerate the recovery of AD data in the face of corruption, accidental deletion, and ransomware attacks by enabling automated forest-level recovery.

Commvault® Cloud Cleanroom™ Recovery

This solution offers a secure, isolated recovery environment on-demand. It allows organizations to test their cyber recovery plans, deliver rapid and clean recovery of applications and data, and perform forensic analysis. With air-gapped storage, built-in automation, and AI-enhanced scaling, Cleanroom Recovery helps maintain continuous business operations despite cyber threats.

Commvault® Cloud Rewind™

Go beyond traditional backup and disaster recovery – with a solution that allows you to continuously discover, protect, recover, and rebuild to establish cyber resilience and maintain continuous business operations. You can rewind to a specific point in time and rapidly rebuild dynamic and distributed cloud applications quickly from outages and ransomware attacks. With a patented dual-vault cloud time machine, you can quickly restore your data, apps, and configurations.

While a disaster recovery plan is essential to protect your company's infrastructure, you **won't be fully protected** unless you also have a cyber recovery plan and testing strategy in place, too. This is critical to keeping both your data and your reputation safe in the face of cyberattacks.

Learn more about how Commvault can help protect your organization, and get a demo of Commvault® Cloud Cleanroom™ Recovery and Cloud Rewind.