Commvault

DISASTER RECOVERY ≠ CYBER RECOVERY

While your organization needs to have a disaster recovery plan to protect your systems, hardware, and data, you can't count on it to help you prepare for the threat of a cyberattack.

Different attacks need different approaches to get you back up and running.

Let's look at the differences and see why a **cyber recovery plan is a critical safeguard.**

01
WHY DO YOU NEED IT?

DISASTER RECOVERY

Needed to handle accidental events like fires, natural disasters, or hardware failures

CYBER RECOVERY

Needed to handle malicious attacks like ransomware or data breaches

02
WHAT DOES RECOVERY ENTAIL?

DISASTER RECOVERY

Predefined plan with established steps to restore systems quickly or failover to backup site

CYBER RECOVERY

Often requires investigation and remediation before recovery; need to contain attack and scrutinize every element before restoring

03
WHAT ARE THE GOALS?

DISASTER RECOVERY

Ensure business continuity, minimize long-term impact, and protect critical data

CYBER RECOVERY

Minimize cyberattack damage, prevent data loss, and maintain security posture

04
HOW DO YOU DO IT?

DISASTER RECOVERY

Full system backups, off-site replication

CYBER RECOVERY

Security information and event management, Commvault Cloud Air Gap Protect, and Cleanroom™ Recovery

05
HOW DO YOU TEST IT?

DISASTER RECOVERY

Simulate scenarios to evaluate if your systems, infrastructure, and personnel can respond and recover promptly

CYBER RECOVERY

A safe and isolated environment where you can test on demand and minimize disrupting production systems

CYBER RECOVERY–READY DESIGN SCOPE

SCENARIOS

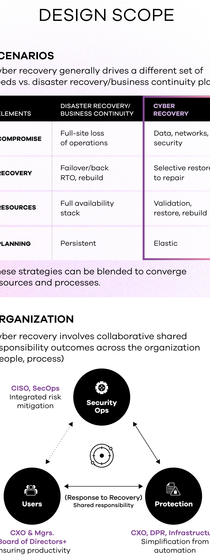
Cyber recovery generally drives a different set of needs vs. disaster recovery/business continuity plans

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

These strategies can be blended to converge resources and processes.

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.

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

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