Commvault

eBOOK

Guide to Cyber Recovery Preparedness

LEARN HOW YOUR COMPANY CAN BE READY FOR THE CHALLENGES THAT COME ITS WAY.

CONTENTS

Many organizations' security, IT, and operations teams have considered cyber recovery and disaster recovery to be the same. However, cyber recovery from recent incidents has revealed some unique curveballs compared to regular disaster recovery. The variability in attacker tactics, techniques, and procedures have shown that cyber recovery plans need to consider:

- **Unpredictability and evolving threats:** Unlike a natural disaster, cyberattacks are malicious and attackers have gone to great lengths to try to hide their actions and movement. Because of this, it can be hard to pinpoint exactly when the attack began, what systems are affected, or the full extent of the damage.
- **Secondary attacks:** Attackers have been seen planting code to launch secondary attacks during the recovery process or creating persistent backdoors that are automatically opened upon a restore action.
- **Compromised backups:** In some cases, attackers have targeted backups specifically to ensure that recovery efforts are ineffective. This makes the need to pay a ransom to recover production data more real.
- **Time constraints:** Businesses often face immense pressure to get back online quickly after a cyberattack. Downtime has been shown to cost an enterprise up to $12 million a day[1]. And to make things worse, rushing recovery can lead to restoring already-compromised systems, further amplifying the damage.
- **Resource drain:** Cyber recovery can be a resource-intensive process, requiring expertise from IT, security, legal, and potentially even law enforcement teams. This can strain already-stretched resources in a company, and can distract security and operations teams from other possible cyber threats.

By understanding these challenges, organizations can use some foundational elements of disaster recovery to build a cyber recovery plan that anticipates these difficulties and helps them bounce back more effectively from an attack.

This guide will help set the stage for your organization's cyber recovery preparedness by giving you concepts, ideas, and processes needed to establish your own program, all while aligning to some commonly observed frameworks.

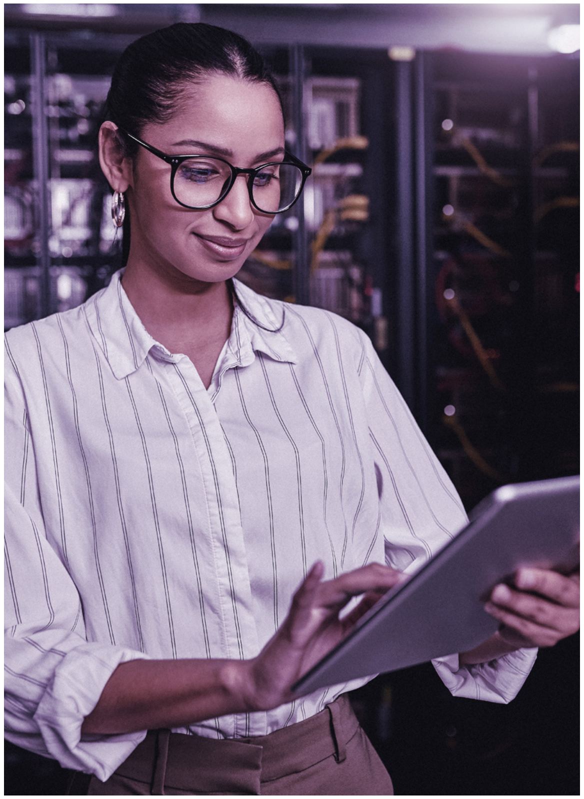
[1] SolarWinds: Pingdom Team, Average Cost of Downtime per Industry, Jan 9, 2023.

NIST CYBER SECURITY FRAMEWORK AS A GUIDE

The Cyber Security Framework from the National Institute of Standards and Technology (NIST CSF) has long been a guiding light for security teams to build and align their security programs and defend against new and evolving cyber threats.

Use Identify, Detect, Protect, Respond, and Recover framework to explain how to build on each for a successful cyber recovery.

1. **Identify.** Understand your data, including sensitive/critical data, where it is, and who's responsible for it.
2. **Detect.** Utilize security controls and technology to observe what's happening to your environment and data.
3. **Protect.** Implement mechanisms to lock down your sensitive or critical data and prepare it for recovery.
4. **Respond.** Remove the attacker from your environment and remove or protect the attack vector used to infiltrate your organization. If this cannot be done quickly, prepare a new, untouched, uncompromised workspace to restore and use to continue operations.
5. **Recover.** Rebuild an uncompromised version of your entire environment, including the data, applications, and infrastructure.



PREPARING FOR THE UNEXPECTED

By their very nature, cyber incidents are often covert attacks orchestrated behind the scenes for days or weeks before destruction or havoc takes place. Studies have shown that the average dwell time – the amount of time an attacker has actually been inside an organization during an attack – is 204 days, or nearly 7 months.[1]

> 204 days, or nearly 7 months
>
> **the average dwell time – the amount of time an attacker has actually been inside an organization during an attack**

Organizations have long conducted penetration tests to highlight areas where their defenses are weak and tabletop exercises to test disaster recovery. But with the variability cyberattacks, the practice needs to take into account that almost nothing can be implicitly trusted in a true cyber recovery scenario. Backups need to be scanned for persistent malware. Infrastructure must be cleaned to confirm only authorized users are present. And applications and data need to be checked for back doors and restored to a pre-attack (or pre-infilitration) state.

[1] 2023 IBM Ponemon Cost of a Data Breach Report, p14 Cost of a Data Breach Report 2023.pdf

REDUNDANCY CAN BE PROHIBITIVELY EXPENSIVE

Having additional dark sites to provide redundancy is a valuable method to protecting your data, giving you a place to practice and prepare for cyberattacks. But, of course, having an additional set of infrastructure comes at an immense cost.

Each physical location requires major expenses like planning, real estate, construction, equipment, energy, taxes, staffing, and ongoing maintenance. Those costs add up quickly and can be in the tens or hundreds of million of dollars each year, depending on the size of the undertaking, making it out of the budget – and out of the question – for many organizations.

ON-DEMAND CLEANROOM RECOVERY

With the advent of Commvault® Cloud Cleanroom™ Recovery, companies can avoid the cost and complexity of managing on-premises cleanrooms. The first and only cleanroom for cyber recovery lets you rapidly test and recover in a safe, cloud-based environment.

Cleanroom Recovery is a practical and affordable solution, making testing and recovery more accessible to more companies. It's also easy to set up on demand and test as needed, making it convenient when you want to make changes or test different scenarios.

You can easily recover applications and data, and conduct forensics after an event. You'll have an isolated recovery environment for business continuity in the event of an attack. Cleanroom Recovery also includes an integration with Microsoft Defender that automates threat scanning to help confirm data is clean.

HOW CLEANROOM RECOVERY PROVIDES A MALWARE-FREE CLOUD ENVIRONMENT

Air-gapping
Isolated data copies, separate from source environments.

Immutable design
Backups with multi-layered zero-trust access controls.

Built-in automation
Leverage automation and orchestration for easy implementation and simple operations.

Resilient ransomware protection and end-to-end security
Built-in anomaly detection, reporting and encryption of data at-rest and in-flight.

Application recovery validation
Data recoverability through orchestrated application recovery validation.

Secure forensic analysis
Perform secure analysis with malware-free hardware in isolated cloud environments.

eBOOK

One certainty in cyber security: Bad actors will continue to innovate to find vulnerabilities. Your best chance to protect your company in the face of cyberattacks is to have a well-thought-out cyber recovery plan that you test often. **Cleanroom Recovery offers a safe, isolated space to test your plan and rapid recovery if trouble does arise.**

Learn more: **www.commvault.com/platform/cleanroom-recovery**

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®