eBOOK

Guide to Cyber Recovery Preparedness

for the Financial Services Industry

LEARN HOW TO REMAIN RESILIENT IN THE FACE OF INCREASING AND EVOLVING CHALLENGES

Commvault + CDW

CONTENTS

CYBER LOSSES ADD UP FOR FINANCIAL INSTITUTIONS

Money makes the world go 'round. It isn't just a cliché: From global markets to large corporations to individual savings, the world of finance impacts everyone. With financial firms holding so much personal data and engaging in such a large volume of transactions, they continue to be an attractive target for cyberattacks.

The problem is staggering: In 2024, 65% of financial organizations were hit by ransomware attacks[1] – with an average recovery cost of $2.58 million.[2]

These organizations also face greater financial impacts than other industries. While the average cost of a breach for all industries is $4.88 million, that rises to $6.08 million for financial firms.[3]

All told, in the span from 2004 – 2023, financial firms reported $12 billion in direct losses from cyber incidents, $2.5 billion of that from 2020 – 2023 alone.[4]

Commvault + CDW

[1] Statista
[2] The State of Ransomware in Financial Services 2024, Sophos.
[3] Cost of a Data Breach Report 2024, IBM.
[4] International Monetary Fund Global Financial Stability Report 2024.

IN FINANCE, CYBER RECOVERY IS COMPLEX

Many organizations' security, IT, and operations teams have considered cyber recovery and disaster recovery to be the same – but a one-size-fits-all approach isn't the answer. Cyber recovery, especially in a highly regulated industry like finance, is more complicated than 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:** Ninety percent of financial services organizations hit by ransomware reported that their backups were targeted.[5] Attackers are also known to attack backups specifically to make recovery efforts ineffective. This makes the need to pay a ransom to recover production data more real.
- **Time constraints:** Financial organizations face immense pressure to get back online quickly after a cyberattack in order to minimize both monetary and reputational damage as well as meet regulatory obligations. Downtime has been shown to cost enterprises an average of $14,056 a minute, rising to $23,750 for large organizations of more than 10,000 employees.[6] And to make things worse, rushing recovery can lead to restoring already-compromised systems, further amplifying the damage.
- **Resource drain:** Cyber recovery at financial firms can be a resource-intensive process, requiring expertise from IT, security, legal, compliance, 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, financial services 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.

[5] The State of Ransomware in Financial Services 2024, Sophos.
[6] Enterprise Management Associates, "IT outages: 2024 costs and containment," Valerie O'Connell, Research Director, April 2024.

NIST CYBERSECURITY FRAMEWORK AS A GUIDE

The Cybersecurity 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. While not a regulatory requirement, it is widely adopted by U.S. financial institutions.

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

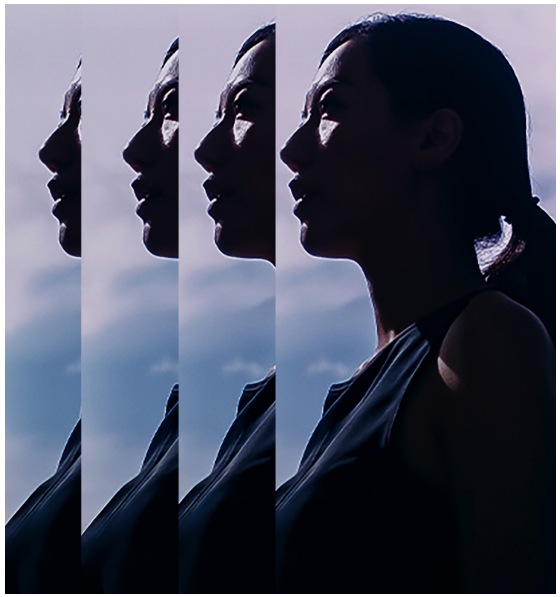
1. **Identify.** Understand your data, including sensitive/critical data, where it is, and who's responsible for it.

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.

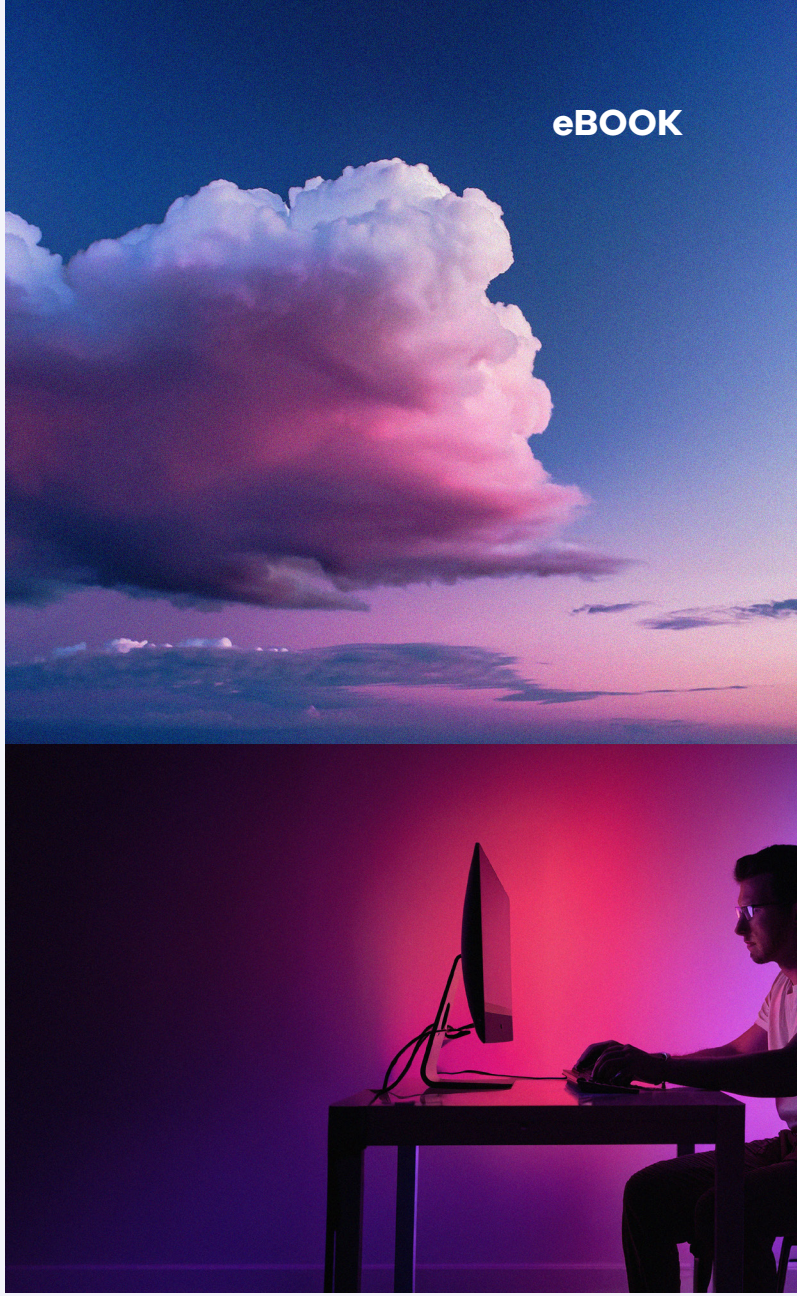
4. **Respond.** Remove the attacker from your environment and remove or protect the attack vector used to infiltrate your organization. If this cannot be done quickly, prepare a new, untouched, uncompromised workspace to restore and use to continue operations.

5. **Recover.** Rebuild an uncompromised version of of your environment, including the data, applications, and infrastructure.



Learn more about recent mandates for financial entities in the European Union in Exploring DORA: A Guide to the Digital Operation Resilience Act. And read up on Australia's Security of Critical Infrastructure Act – which aims to protect critical assets across 11 industries, including the financial sector – in A Guide to the SOCI Act.

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.

> ## 194 days, or more than 6 months
>
> **the average dwell time – the amount of time an attacker has actually been inside an organization during an attack**[7]

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 in 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-infiltration) state.

[7] Cost of a Data Breach Report 2024, IBM.

MINIMUM VIABILITY: THE FIRST STEP TO CYBER RECOVERY

Once your company has been hit by a cyberattack, you're under immense pressure to return to business as usual as soon as possible. The best way to resume operations quickly? Just restore to minimum viability – the most critical assets you need to maintain continuous business. That way, you can continue to carry on the most vital aspects of your organization while a full restoration is underway.

Once you identify your most critical systems, processes, and data that will enable you to return to minimum viability, you'll need to make a plan for how you will restore them in the event of an incident. You need to understand the impact of downtime, and you must test and update your plan as needed.

Read The Ultimate Guide to Minimum Viability to learn more about the steps to restore your business operations and our recommended practices.

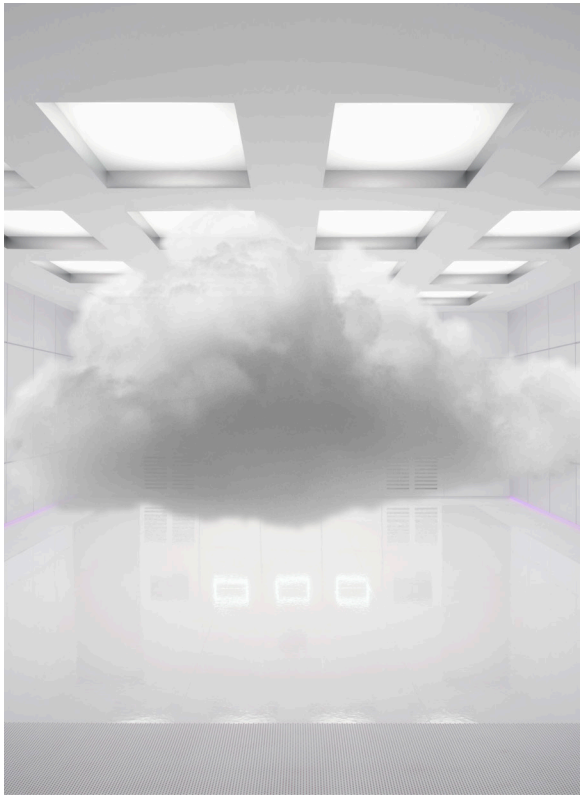
THE FASTEST, MOST COMPLETE CYBER RECOVERY

Commvault provides solutions to protect, test, and recover your data, apps, and workloads – delivering comprehensive recovery and true cyber resilience.

Commvault® Cloud Cleanroom™ Recovery lets you test and recover in a safe, on-demand, cloud-based environment. 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.

Commvault Cloud Rewind™ automatically writes code to recover data and rebuild cloud applications in near–real time so you can be back in business within minutes of a failure – all without the need for manual intervention.

Commvault Cloud for Active Directory Enterprise Edition delivers rapid recovery for AD and Entra ID environments. It helps automate and orchestrate the recovery of forest-level ADs after an incident, enabling you to get back to minimum viability quickly.



eBOOK

One certainty in cyber security: Bad actors will continue to innovate to find vulnerabilities. Your financial organization can stay one step ahead with a well-thought-out cyber recovery plan and strategy to **protect your assets and maintain continuous business in the face of threats.**

To learn more, visit **cdw.commvault.com**

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

Commvault® + CDW