SHI | COHESITY

Beyond prevention: Ransomware resilience for financial services

A practical guide to ransomware readiness and rapid recovery

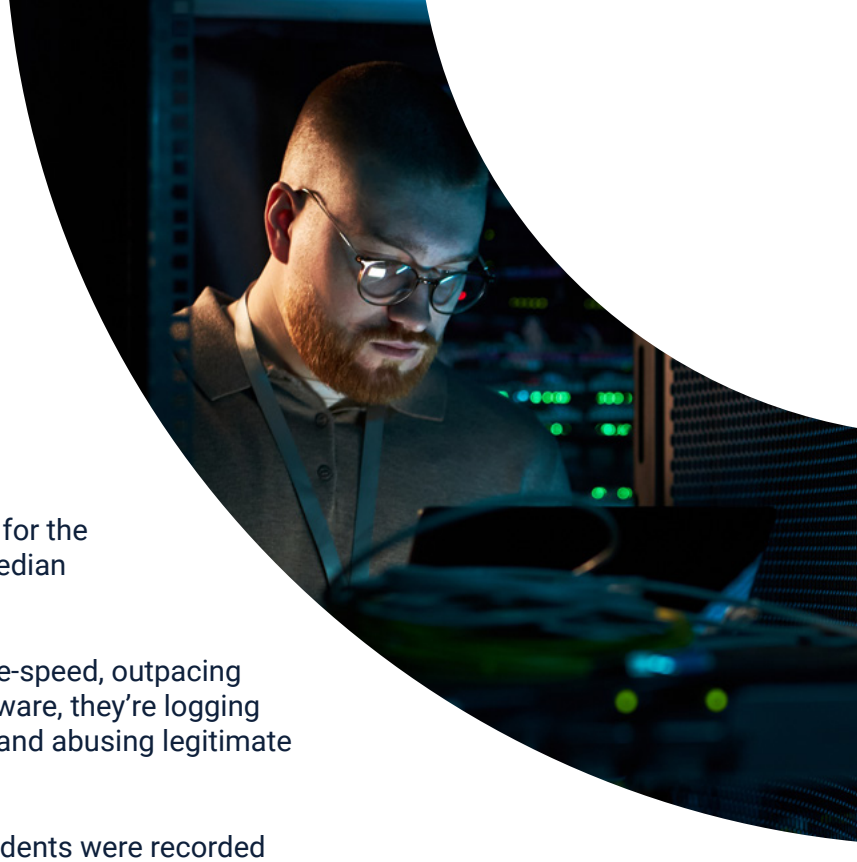


Table of contents

Executive summary	**3**
Ransomware in the financial sector	**4**
What readiness requires	**6**
Best practices for resilience	**7**
• Assess your current state	**7**
• Establish a secure recovery zone	**8**
• Transition to active defenses	**9**
• Stop treating resilience like an IT problem	**11**
• Run continuous recovery simulations	**12**
Implementing resiliency best practices with SHI and Cohesity	**13**
Starting your resilience journey	**15**



SHI | COHESITY



Executive summary

Ransomware has escalated into a high-stakes crisis for the financial sector, which currently faces the highest median ransomware demands of any industry at $3 million.[1]

Threat actors are weaponizing AI to move at machine-speed, outpacing traditional defenses. Instead of breaking in with malware, they're logging in with valid credentials, hijacking trusted identities, and abusing legitimate system tools to blend in and navigate environments.

The momentum is undeniable: 65 finance-sector incidents were recorded in Q1 2026 alone, a 76% increase over Q1 2025.[2]

As attacks become faster and more scalable, the challenge is no longer stopping every threat. It's building resilient systems that can withstand continuous pressure and recover quickly when an incident occurs.

> "By 2028, 50% of CISOs will be asked to own disaster recovery, in addition to incident response, reflecting a broader organizational focus on cyber resilience."[3]

This ebook details five best practices financial organizations can use to rethink ransomware readiness and strengthen cyber resilience with a proactive approach that balances people, process, and technology.

[1] Sophos, *The State of Ransomware in Financial Services 2025:* https://assets.sophos.com/X24WTUEQ/at/749t28qhvtxq93p8gb7wtgz/sophos-state-of-ransomware-in-financial-services-2025.pdf

[2] Black Kite Research Group, *2026 Financial Services Cybersecurity Report:* https://blackkite.com/reports/2026-financial-services-report

[3] Gartner "Predicts 2026: Cybersecurity Program Rebrands to Cyber Resilience," Arthur Sivanathan, Charlie Winckless, and Will Candrick, December 11, 2025

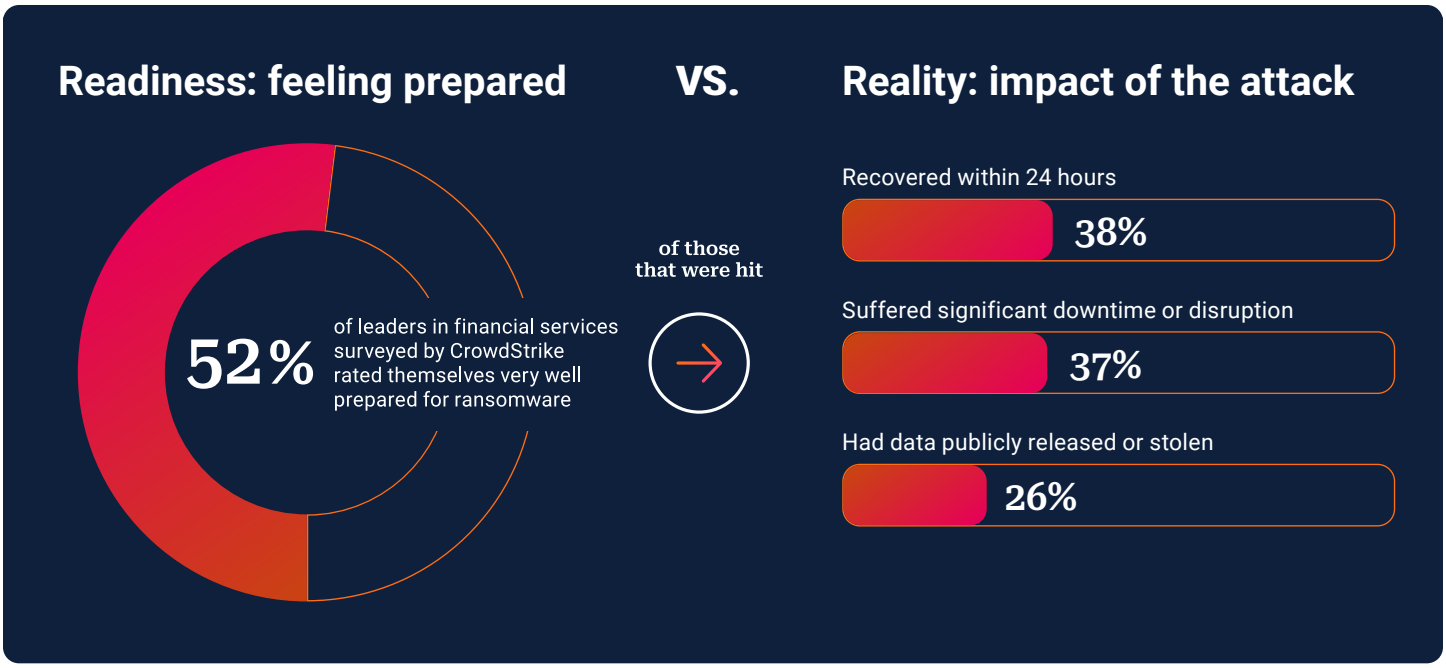
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates.



Ransomware in the financial sector

Trust is everything in financial services. Your customers, investors, and regulators expect money and sensitive data to be protected. Maintaining their trust in an era defined by AI-driven threats and identity-led attacks isn't easy.

Many financial services organizations feel prepared, but most aren't as ready as they think.



According to CrowdStrike's State of Ransomware Survey 2025, 52% of senior IT and cybersecurity decision-makers in financial services rated themselves "very well-prepared" to defend against ransomware. Of those that were hit, only 38% recovered within 24 hours, 37% suffered significant downtime or disruption, and 26% had data publicly released or stolen.[4]

[4] CrowdStrike, *State of Ransomware Survey:* https://www.crowdstrike.com/en-us/resources/reports/state-of-ransomware-survey/

“

Ransomware doesn’t wait for a convenient time, and neither should your recovery. The organizations best positioned to withstand an attack are those that have validated that their data is clean and their systems can come back online fast. A resilient storage foundation provides that certainty, giving teams confidence instead of hope.

Joye Purser
Field CISO, Cohesity



What readiness requires

Disaster recovery and ransomware recovery aren't the same

Traditional disaster recovery was designed to address physical or operational disruptions such as power outages, hardware failures, or natural disasters. It assumes that data remains trustworthy, and business can resume as soon as impacted systems come back online.

Ransomware breaks that assumption.

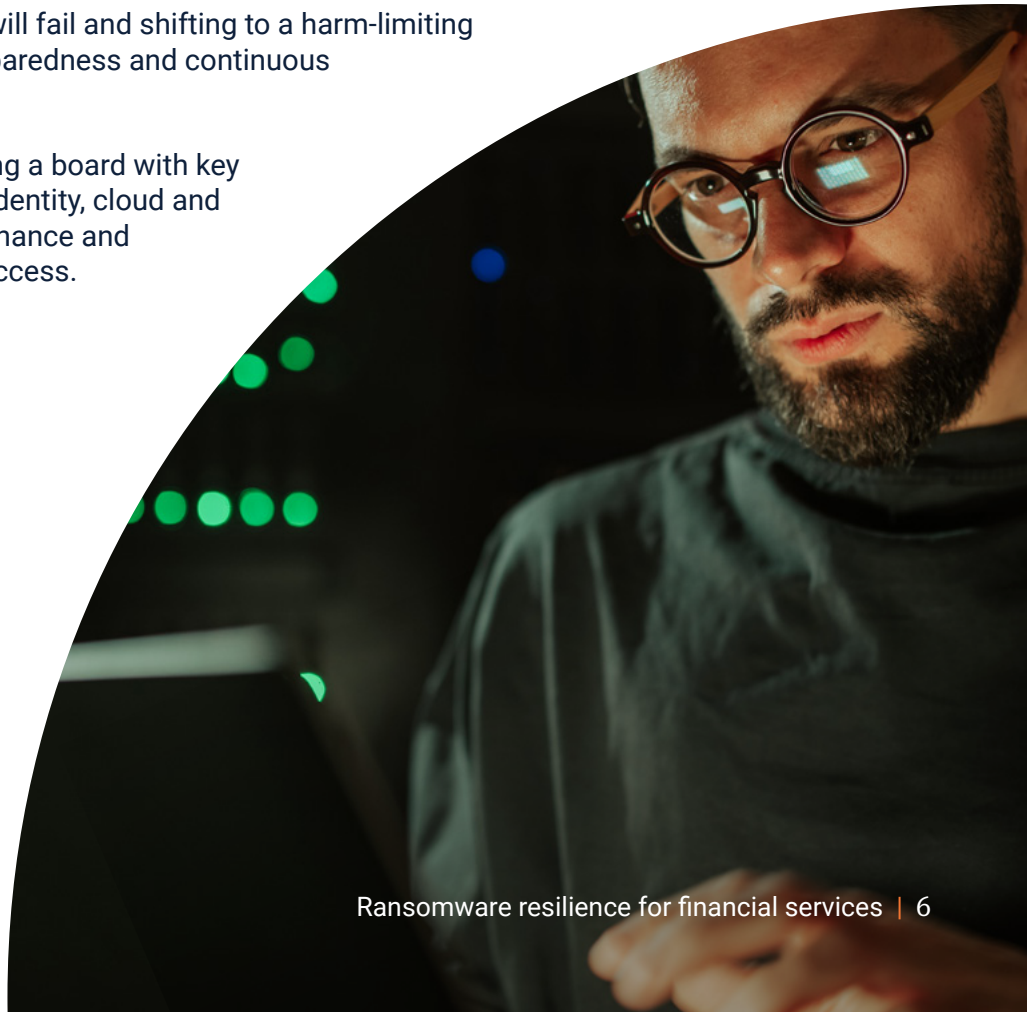
Ransomware involves an active and unpredictable attack on data and infrastructure. Data integrity can't be trusted. Identity systems can be compromised. Backups may contain malware; replication can spread the infection, introducing hidden threats to recovery environments.

Not all attacks can be prevented. Even if your organization has mature disaster recovery processes in place, you can't rely on the same mechanisms to recover from ransomware.

Boards, cyber insurers, and regulators no longer accept "we have backups" as a strategy for handling ransomware. Financial services organizations need verifiable recovery readiness to support strict regulatory compliance requirements.

This means accepting that prevention will fail and shifting to a harm-limiting approach that prioritizes proactive preparedness and continuous recovery testing.

A successful program considers building a board with key team membership from data security, identity, cloud and data center storage, compliance, governance and business team leadership to ensure success.



Best practices for resilience

1. Assess your current state

Conduct a security posture review to evaluate current defenses and identify gaps in policies, processes, and technical controls, focusing on the following core areas.

☑ **Identity and Access Management (IAM)**
Look for phishing-resistant multi-factor authentication (MFA) across all administrative and user portals, and review least-privilege access rules. Ensure high-value identity provider (IdP) platforms and configuration snapshots are integrated into your resilience plan to protect against disruption or compromise.

☑ **Backup and Recovery**
Determine whether critical data backups are immutable, isolated through air-gapped storage or vaults, and tested for rapid restoration timelines.

☑ **Data classification**
Catalog and tag data assets based on business sensitivity, compliance mandates, and operational value to support the right level of protection for critical financial records and customer information. Integrate these prioritized assets directly into your recovery strategy, ensuring continuous updates and testing.

☑ **Network Segmentation**
Evaluate how well sensitive systems are isolated from general corporate networks to limit lateral movement in the event of an intrusion.

☑ **Incident Response**
Test operational readiness through tabletop exercises mapped to security industry best practices such as the NIST Cybersecurity Framework.

☑ **Vulnerability Management**
Assess patching cadence for internet-facing edge devices, firewalls, and virtual private network (VPN) gateways. Identify specialized AI tools that can help establish automated remediation loops.

The results of this assessment will help you map business-critical data, applications, and infrastructure.

> The average time between the disclosure of a vulnerability and its first exploitation has fallen to a single day (a zero-day event), leaving companies little more time to react than residents of tornado alley. Even when patches exist, companies often don't respond in time: in ~60% of breaches, a patch was already available at the time of compromise. For software developers and maintainers, the most important epiphany is the following: the same tools that are used to detect and exploit vulnerabilities can also be used to propose code fixes and remediate them. Claude Security, GPT 5.5-Cyber and OpenAI's Codex Security Plugin are notable examples.[5]

[5] JP Morgan, Patchmageddon: https://privatebank.jpmorgan.com/content/dam/jpm-pb-aem/global/en/documents/eotm/patchmageddon.pdf

2. Establish a secure recovery zone

Build a secure, off-site recovery zone that includes an isolated clean room and a minimum viable recovery environment (MVRE).

Clean room

A clean room provides the air-gapped computing power and storage you need for investigation and staging. Be sure to:

☑ **Establish network isolation**
Provision a dedicated cloud account (e.g., in AWS or Azure) that is separated from your primary enterprise networks to prevent adversaries' lateral movement.

☑ **Enforce identity segregation**
Lock down the environment with distinct, independent identity controls and MFA separate from your production Active Directory.

☑ **Employ pre-stage forensics tools**
Create an immutable "digital jump bag" — a hardened, read-only file share that's pre-loaded with security tools, scanners, and known-good software configurations.

☑ **Implement data ingress sanitization**
Deploy automated, offline malware scanner pipelines at the clean room perimeter to scrub and validate compromised backup images before they're mounted for recovery.

Minimum viable recovery environment

An MVRE is an infrastructure footprint containing the bare-minimum "Tier 0" assets you need to make your business operational. This is what should be recovered immediately following a confirmed incident. Here's how to create an MVRE:

☑ **Map core infrastructure dependencies**
Identify core dependencies such as Active Directory, Domain Name System (DNS), and fundamental routing rules.

☑ **Isolate vital security controls**
Include your core endpoint detection, network firewalls, and logging tools so your incident response team has visibility the moment systems boot up.

☑ **Automate the recovery sequence**
Script the precise order of operations. Identity systems should boot first, followed by infrastructure services, and finally your most critical line-of-business applications.

☑ **Enforce strict egress filtering**
Block all outbound internet access by default, allowing only connections to pre-verified vendor update sites to prevent compromised assets from calling home to command-and-control servers.

3. Transition to active defenses

Shift from traditional backup and recovery toward active defense at the storage layer.

Prioritize solutions that provide the following capabilities:

☑ **Data-layer active detection and continuous classification**
Leverage AI and machine learning to analyze backup data at ingest. The platform must look for behavioral anomalies such as entropy spikes, mass deletions, and suspicious file extensions directly within snapshots. Technologies such as data security posture management (DSPM) within your data security program will be required.

☑ **Automated threat response**
Flag real-time attacks, immediately alerting operations teams and triggering API-driven playbooks to isolate compromised credentials and contain the impact. Ensure Identity Threat Detection and Response (ITDR) capabilities are in place to support this effort from within the Identity Management team.

☑ **Recovery assurance**
Scan immutable snapshots cleanly in an isolated sandbox using integrated threat feeds and deployed technologies that will ensure identity and data recovery for the organization, pinpointing clean recovery points before data is restored into production.

☑ **SIEM/SOAR integration**
Centralize data visibility by feeding storage threat signals directly into enterprise tools. Bidirectional API extensions allow security operations teams to orchestrate and track ransomware response from a single pane of glass.

☑ **Zero trust architecture and storage hardening**
Secure the underlying backup architecture with immutable file systems, DataLock (WORM) parameters, role-based access control, and multi-user quorum authorization to guarantee that adversaries cannot delete or modify secondary data repositories. Extend microsegmentation capabilities where applicable to isolate backup environments and prevent lateral movement during an attack.

Look for solutions that bring these capabilities together as an integrated solution rather than relying on disconnected tools, teams, and manual processes.

“

Organizations should no longer consider cyber resilience as an IT operation and should be focusing on this as a business survival mandate. CISOs and business leaders should continuously assess and manage risk while increasing organizational resilience.

The output of this exercise should support and adjust clean room strategies and minimum viable recovery points. Building the right team and choosing the right technology is a must to build a trusted secure recovery foundation.

David O’Leary
Field CISO, SHI



4. Stop treating resilience like an IT problem

Treat cyber resilience like a shared responsibility and align governance models with business outcomes. Key actions include:

☑ **Manage board-level financial and business expectations**
Shift conversations with the board away from stopping all breaches to establishing acceptable downtime metrics and evaluating the financial exposure of disrupted transaction ledgers instead.

☑ **Initiate cross-functional ownership**
Collaborate closely with legal, procurement, and risk departments to automate the accelerated 36-to-48-hour incident reporting timelines required by regulators and frameworks, including the Securities and Exchange Commission (SEC), Federal Deposit Insurance Corporation (FDIC), Federal Financial Institutions Examination Council (FFIEC), and Digital Operational Resilience Act (DORA).[6]

☑ **Prepare for crisis communications management**
Deliver factual updates to the press to stop damaging speculation, coordinate data-breach disclosures to affected customers, and proactively engage regulators, cyber insurance carriers, law enforcement, national computer emergency response teams (CERTs), and FS-ISAC.

☑ **Align budget and recovery metrics**
Hold line-of-business executives accountable for their own uptime by mapping department funding directly to the cost of conducting localized, non-disruptive tabletop simulations.

[6] U.S. Securities and Exchange Commission, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure:* https://www.sec.gov/rules-regulations/2023/07/s7-09-22

5. Run continuous recovery simulations

Conduct recovery drills, backup testing, and training to ensure your organization responds as quickly as possible. Here's how:

☑ **Conduct adversarial simulations**
Work with internal red teams or external partners to run unannounced ransomware simulations that help teams actually spin up the MVRE.

☑ **Establish out-of-band communications**
Train and equip your IT, incident response, and executive teams to communicate out-of-band when primary email and chat systems are unavailable.

☑ **Audit recovery time metrics**
Treat recovery testing as an auditable performance indicator. Measure the exact time it takes to detect an anomaly, isolate the threat, and restore a core ledger to verify that your actual recovery timeline matches your regulatory requirements.

☑ **Introduce failures**
Purposefully inject unexpected infrastructure failures, such as corrupted hypervisors, expired encryption keys, or unresponsive third-party APIs, into simulations to test your team's ability to pivot to secondary out-of-band recovery playbooks.



Implementing resiliency best practices with SHI and Cohesity

SHI and Cohesity help financial services organizations put these ransomware resilience best practices into action.

Best practice	Issue	Our solution
Assess your current state	Many organizations struggle to fully understand where sensitive data resides and whether it is adequately protected across increasingly complex hybrid environments.	Cohesity helps close this visibility gap by continuously scanning backup data with Cohesity DSPM, identifying sensitive and poorly secured data across on-premises, cloud, and SaaS environments without touching production systems. These insights can strengthen your understanding of where risk exists and support more informed resilience decisions.
Establish a secure recovery zone	A recovery zone is only effective if you can confidently access clean data and quickly validate recovery processes during an incident.	Cohesity FortKnox delivers an air-gapped, immutable copy of data in a Cohesity-managed cloud vault. Cohesity's built-in clean room capability further supports recovery readiness by enabling teams to instantiate historical snapshots via API to investigate incidents without touching production systems, turning the "digital jump bag" concept into a repeatable, orchestrated workflow rather than a manual one.
Transition to active defenses	Moving from siloed tools toward unified solutions that broaden visibility across cloud, identity, and data is critical.	The Cohesity Data Cloud embodies this modern approach by applying machine learning directly to backup data at ingest to flag entropy spikes, mass deletions, and other anomalies. It also integrates with Data Security Alliance partners, such as CrowdStrike Falcon and Google Threat Intelligence, to pinpoint clean recovery points before data is restored to production. Cohesity's Quorum capability enforces multi-user authorization on backup and recovery tasks, and DataLock (WORM) protections prevent even privileged accounts from deleting secondary data.

The IBM Cost of a Data Breach Report 2026 found that platform-native automation slashed breach detection and containment timelines by 65 days, and AI-driven security platforms saved an average of $1.93 million per breach.[7]

[7] IBM, *Cost of a Data Breach Report 2026:* https://www.ibm.com/reports/data-breach

Best practice	Issue	Our solution
Stop treating resilience like an IT problem	Effective cross-functional response depends on quickly understanding which data and systems were affected so business, legal, risk, and compliance teams can make informed decisions.	When an incident is declared, Cohesity DataHawk can automatically identify impacted backed-up systems and data, giving these teams the evidence they need to meet accelerated regulatory reporting requirements such as those imposed by the SEC, FFIEC, and DORA.
Run continuous recovery simulations	Recovery simulations are most effective when they mirror the processes, tools, and decision-making workflows your teams would use during an actual ransomware event.	Cohesity CERT gives your team direct access to incident response experts during a live event, while Cohesity's orchestration engine automates and rehearses recovery sequencing. This includes standing up an MVRE, so simulations reflect the same automated playbooks you'd run in a real attack.

SHI makes Cohesity Data Cloud work in your environment, assessing your security posture, evaluating fit, planning deployment, integrating with existing operations, and establishing governance so recovery stays predictable. From the design stage to ongoing optimization, our focus is on reducing downtime risk, lowering operational overhead, and keeping your data protected.

Starting your resilience journey

Are you ready for ransomware?

Financial services organizations that cling to outdated prevention-only models will find themselves unprepared for successful attacks, resulting in greater monetary and reputational damage.

True resilience requires more than prevention. By assessing your current posture, establishing a secure recovery zone, implementing a modern backup and data protection solution, collaborating with the right people, and running continuous simulations, you can withstand, respond to, and recover from attacks.

Build ransomware readiness with **SHI** and **Cohesity.**

Let us show you how.

- Schedule an SHI-funded Security Posture Review
- Learn more about Cohesity Data Cloud
- Contact us for more information

