

EXECUTIVE PAPER · DISASTER RECOVERY

Ransomware Readiness Is a Recovery Problem

Boards that measure ransomware readiness by prevention spend are missing the variable that decides whether the company pays. Here is how to fund and test the ability to rebuild.

AUTHOR

Chris Watkins

SERVICE

Disaster Recovery

FOR

CEO, Board · 11 min read

AT A GLANCE

The problem. Most ransomware programs are judged by how well they keep attackers out. The outcome that matters to the board is how fast the company can run again without paying. In a 2024 survey of almost 3,000 victims, recovery cost eight times more when attackers had reached the backups, and attackers tried to reach them in 94% of cases.

Why it persists. Prevention is easy to buy and easy to report. Recovery is hard to see until the day it is needed. Backups often share credentials, networks, and administrators with the systems they protect, so the same intrusion that encrypts production can lock the copies.

The recommendation. Fund four recovery conditions and ask for evidence on each: copies the attacker cannot reach, a recovery path isolated from the compromised environment, credentials hardened so a stolen password or a help desk call cannot open everything, and a clean rebuild the team has performed under time pressure. Treat the ability to refuse payment as a board-level metric.

The Decision in Front of You

Every board will eventually face a ransom demand, either at its own company or at a supplier the business cannot run without. The decision that matters is made long before that call. It is whether the company has paid for the ability to recover on its own.

Sophos's 2026 survey of 2,158 ransomware victims across 17 countries found that 56% of attacks succeeded in encrypting data, and 48% of organizations with encrypted data paid the ransom [1]. The median payment was $769,000, and the average recovery cost, excluding any ransom, was $1.7 million per incident [1]. A year earlier the median payment was $1 million and the median recovery cost $1.53 million [2].

The ransom is the smaller number. Recovery cost, lost revenue, and weeks of manual operations are where boards lose money, and all of them depend on how quickly the company can rebuild from something it trusts.

What's Happening

Attackers go after the backups first

Sophos asked 2,974 victims in early 2024 whether attackers had tried to compromise their backups. Ninety-four percent said yes, and 57% of those attempts succeeded [3]. Victims whose backups were compromised paid the ransom 67% of the time, against 36% for those whose backups survived. Their

median recovery cost was $3 million, eight times the $375,000 reported by victims with intact backups [3].

The two most recent annual surveys show some improvement and a stubborn gap.

Exhibit 1. Payments are falling and backup use is rising, yet a third of victims still cannot restore from their own copies

Measure	2025 survey	2026 survey
Respondents (ransomware victims, 17 countries)	3,400	2,158
Attacks that encrypted data	about 50%	56%
Victims with encrypted data who restored from backups	54%	66%
Victims with encrypted data who did not restore from backups	46%	34%
Median ransom payment	$1.0 million	$769,000
Recovery cost per incident, excluding ransom	$1.53 million (median)	$1.7 million (average)

Source: Sophos, The State of Ransomware 2025 [2] and 2026 [1]. The 2025 recovery figure is a median and the 2026 figure an average, so the two are not directly comparable. The "did not restore" row is the complement of the row above it.

The 2025 backup figure was the lowest in six years [2]. Even after the 2026 rebound, one encrypted victim in three did not restore from its own backups [1].

Identity is the front door

Sophos classified 79% of the ransomware attacks in its 2026 survey as starting with an identity-based approach, such as phishing, stolen credentials, or brute force [1]. Its companion review of 661 incident response cases found multifactor authentication (a second proof of identity beyond a password) missing where it mattered in 59% of cases [1]. Partial coverage leaves gaps attackers find: 97% of victims whose root cause was compromised credentials had MFA enabled in some form [1].

IBM's 2026 Cost of a Data Breach study reported that 39% of organizations said ransomware hit their systems, the fourth straight year of increases, according to a law firm's summary of the report [4]. In 41% of those attacks, the attackers also went after the victim's brand, through leak sites and public shaming [4].

Three recent cases

Change Healthcare, 2024. On February 12, 2024, attackers used stolen credentials to log into a Citrix remote access portal that had no multifactor authentication. They moved through the network for nine days, took data, and then deployed ransomware [9]. The company's policy required MFA on external systems; this portal was the exception [10]. UnitedHealth's CEO told Congress that the backup systems

were locked up as well, because the primary and backup environments were not isolated from each other, and the company rebuilt the platform from scratch [10]. A ransom of $22 million was paid, and some stolen data still appeared online afterward [12]. UnitedHealth reported a 2024 impact of $3.09 billion, including $867 million in business disruption, and advanced $9.03 billion in loans to providers whose payments had stopped [11].

Marks & Spencer, 2025. The retailer disclosed an attack on April 22, 2025, reportedly begun by impersonating staff to IT help desk workers [13][14]. Online sales of clothing and home goods stopped for weeks and were not expected back until July [14]. Statutory profit before tax for the half year to September 2025 fell from £391.9 million to £3.4 million. One-off incident costs reached about £102 million in that half, with £34 million more expected, partly offset by a £100 million insurance recovery [13].

Jaguar Land Rover, 2025. JLR announced an attack on September 2, 2025, shut down its IT systems, and halted vehicle production at its UK plants for about five weeks [15][16]. A phased restart began around October 8 [16]. The company booked £196 million of direct cyber costs in its July to September quarter [16]. The independent Cyber Monitoring Centre estimated the total cost to the UK economy at £1.9 billion, affecting more than 5,000 organizations, and the UK government underwrote a £1.5 billion loan guarantee to keep the supply chain solvent [15].

The entry points differed: a remote access portal, a help desk, and an intrusion claimed on Telegram by a group calling itself Scattered Lapsus$ Hunters [16]. The weeks of disruption in all three came from rebuilding systems the business could trust again.

SIDEBAR: PAYING DOES NOT END THE INCIDENT

A payment buys a decryption key and a promise. The systems still have to be rebuilt, and the stolen data stays in the attacker's hands. UnitedHealth paid and still saw data surface [12]. US Treasury guidance warns that paying a sanctioned group can violate sanctions law under strict liability, meaning no proof of intent is needed. The same guidance lists offline backups and tested incident response plans among the steps it weighs in a company's favor [8].

Why the Usual Approach Fails

Ransomware budgets tend to flow toward prevention: email filtering, endpoint detection, patching. All of that is necessary. The weakness is that prevention is scored on attacks stopped, and the board has no measure for the attack that gets through.

Several patterns repeat in the public cases.

Backups live inside the blast radius. Backup servers are often joined to the same directory, managed by the same administrator accounts, and reachable on the same network as production. An attacker who holds domain administrator rights can delete snapshots and encrypt the backup catalog with the same keystrokes used on everything else. Change Healthcare's shared primary and backup environments are the public example [10].

The recovery plan assumes a working identity system. Most restore procedures begin with an administrator logging in. If the directory service is compromised, there is nobody the team can trust to log in, and restoring it from a backup may restore the attacker's accounts along with it.

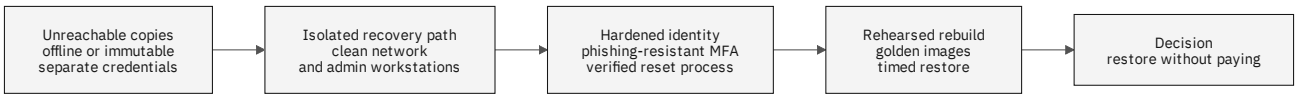
Credential hardening stops at the login page. M&S shows that the password reset process is itself a credential [13]. A help desk that can reset an administrator's MFA after a convincing phone call is an open door, however strong the authentication behind it.

Recovery is untested at scale. Restoring one file proves the backup software works. It says nothing about rebuilding hundreds of servers in the right order, with clean images, while the incident response firm is still investigating.

The Framework: Four Recovery Conditions

The question for the board is whether the company can bring its critical services back without the attacker's cooperation, and how long that takes. Four conditions determine the answer. Each needs a named owner and evidence the board can review.

Exhibit 2. Four recovery conditions decide whether paying is optional



Source: author's framework, drawing on the CISA #StopRansomware Guide [5], NIST IR 8374 Rev. 1 [6], and NIST SP 1800-11 [7].

Unreachable copies. Keep at least one copy of critical data and system configurations that the production environment cannot alter. CISA, the NSA, and the FBI recommend offline, encrypted backups that are tested for availability and integrity, and warn that many ransomware variants hunt for reachable backups to delete or encrypt them [5]. Immutable cloud storage, which cannot be changed until a retention period expires, is an acceptable alternative if configured with care [5]. The copies must sit under different administrator credentials than production. A backup that a stolen domain admin password can delete does not meet this condition.

Isolated recovery path. Plan where the rebuild will happen. That means a network segment, administrator workstations, and tooling that the attacker has never touched. CISA recommends keeping source code, executables, and infrastructure-as-code templates (scripts that rebuild servers and cloud resources automatically) offline alongside the backups, and retaining the hardware needed to restore them [5]. Restoring into the environment the attacker still controls invites a second encryption.

Hardened identity. Require phishing-resistant MFA on email, remote access, and every account that touches critical systems; separate administrator accounts from everyday ones; restrict who can sign in to domain controllers; and audit privileged accounts every quarter [5]. Add a verified process for MFA and password resets that cannot be completed on the strength of a phone call. Plan to rebuild the directory service itself from a known-good state, because recovering anything else depends on it.

Rehearsed rebuild. Maintain golden images, which are preconfigured, current templates of critical systems that can be deployed quickly [5]. NIST's guidance on recovering from ransomware stresses that restored data must be accurate, complete, and free of malware [7], so the rebuild includes checking what you restore. Then time it. The board should know the measured hours to restore identity, then the top five business services, from the isolated copies, performed by the people who would do it on the day.

NIST's 2026 ransomware profile maps these outcomes to the Cybersecurity Framework 2.0 and is a reasonable checklist for auditors and insurers [6].

Costs, Risks, and Tradeoffs

Exhibit 3. What recovery readiness costs, and when it is the wrong priority

Area	Cost or risk	Mitigation
Storage	A second, isolated copy with long retention adds storage and licensing cost	Limit long retention to critical systems; tier older copies to cheaper media
Operations	Separate admin credentials and offline copies slow routine work	Automate backup verification; keep the separate credentials in a sealed break-glass process
Rebuild tests	Timed restores take staff off project work for days each year	Rotate which services are tested; start with identity and the top revenue service
Help desk friction	Stricter identity checks on resets frustrate staff and executives	Publish the process; give executives no exceptions, since attackers impersonate them first
False confidence	Immutable storage can be misconfigured, and a passed test can go stale	Re-test after major changes; have a party outside the backup team verify
When this is wrong	A small firm running almost entirely on SaaS has little infrastructure to rebuild	Focus on account security, SaaS data export or third-party backup, and vendor recovery commitments in contracts

Source: author's analysis; mitigation practices drawn from CISA [5].

How to Act

Exhibit 4. A one-year roadmap to a recovery the board can verify

Window	Actions	Owner	Milestone
First 30 days	Name the services the company cannot operate without. Confirm whether backups for each can be deleted or encrypted using production administrator accounts. List every remote access path and whether it enforces MFA.	CIO with CISO	Written answer for each critical service; list of remote access paths lacking MFA
First 30 days	Agree in advance who decides on payment, with legal counsel and insurer contacts identified, and how law enforcement will be notified [8].	CEO with General Counsel	Decision authority recorded and approved in writing
First 90 days	Create an immutable or offline copy of critical data and configurations under separate credentials. Enforce phishing-resistant MFA on all remote access and privileged accounts. Change the help desk reset process to require verification beyond a phone call.	CISO with infrastructure lead	No critical backup reachable with production credentials; MFA coverage of remote access at 100%
First 90 days	Build golden images for the directory service and the top five services. Perform the first timed restore of identity into an isolated environment.	Infrastructure lead	Measured restore time for identity, reported to the CEO
First 365 days	Timed clean rebuild of the top five services from isolated copies, repeated twice a year. Map controls to NIST IR 8374 Rev. 1 for audit and insurance renewal.	CIO with internal audit	Rebuild of top five services completed within the target the board set; results reported to the audit or risk committee

Source: author's recommendation.

Questions to Ask Your Team

1. If an attacker held our domain administrator password tonight, which backups could they delete?
2. Where would we rebuild if we could not trust any machine on our network?
3. Which remote access paths do not require MFA today?
4. What would our help desk do if someone claiming to be me called to reset my MFA?
5. How many hours did our last full restore of the directory service take, and when was it?
6. Which five services do we restore first, and in what order?
7. Who has authority to decide on a ransom payment, and who do they call first?

8. What evidence would we give our insurer and auditors that our backups are isolated?

Closing

The decision to pay a ransom is made by engineering choices the company made years earlier. Companies whose backups were reached paid at almost twice the rate of those whose backups survived, and spent eight times as much getting back to work [3]. Keep funding prevention, and add the four recovery conditions alongside it. Require a timed rebuild each year and report the hours it took to the board as the measure of ransomware readiness.

Sources

[1] Sophos. "The State of Ransomware 2026." 2026. https://www.sophos.com/en-us/blog/sophos-state-of-ransomware-2026.

[2] Sophos. "Nearly Half of Companies Opt to Pay the Ransom, Sophos Report Finds." Press release, The State of Ransomware 2025. 2025. https://www.sophos.com/it-it/press/press-releases/2025/06/nearly-half-companies-opt-pay-ransom-sophos-report-finds.

[3] Sophos. "The Impact of Compromised Backups on Ransomware Outcomes." 2024. https://www.sophos.com/en-us/blog/the-impact-of-compromised-backups-on-ransomware-outcomes.

[4] Baker Donelson. "Ten Takeaways from IBM's 2026 Cost of a Data Breach Report." Summary of IBM Cost of a Data Breach Report 2026. 2026. https://www.bakerdonelson.com/ten-takeaways-from-ibms-2026-cost-of-a-data-breach-report.

[5] Cybersecurity and Infrastructure Security Agency, MS-ISAC, NSA, and FBI. "#StopRansomware Guide." Updated 2023. https://www.cisa.gov/stopransomware/ransomware-guide.

[6] National Institute of Standards and Technology. "Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile." NIST IR 8374 Rev. 1. 2026. https://csrc.nist.gov/pubs/ir/8374/r1/final.

[7] National Institute of Standards and Technology, National Cybersecurity Center of Excellence. "Data Integrity: Recovering from Ransomware and Other Destructive Events." NIST SP 1800-11. 2020. https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/recover.

[8] U.S. Department of the Treasury, Office of Foreign Assets Control. "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments." 2021. https://ofac.treasury.gov/media/912981/download.

[9] TechTarget. "Change Healthcare breached via Citrix portal with no MFA." 2024. https://www.techtarget.com/cybersecurity/news/366582824/Change-Healthcare-breached-via-Citrix-portal-with-no-MFA.

[10] Cybersecurity Dive. "Change Healthcare cyberattack: 5 technical takeaways from UnitedHealth CEO's testimony." 2024. https://www.cybersecuritydive.com/news/unitedhealth-change-attack-tech-takeaways/715200/.

[11] Becker's Hospital Review. "The financial toll of the Change Healthcare hack: 7 numbers." Reporting UnitedHealth Group year-end 2024 results. 2025. https://www.beckershospitalreview.com/cybersecurity/the-financial-toll-of-the-change-healthcare-hack-7-numbers.html.

[12] Healthcare Dive. "UnitedHealth's cyberattack response costs to surpass $2.3B this year." 2024. https://www.healthcaredive.com/news/unitedhealths-cyberattack-response-costs-to-surpass-23b-this-year/721431/.

[13] ITPro. "M&S reveals massive financial hit from cyber attack." 2025. https://www.itpro.com/security/cyber-attacks/m-and-s-reveals-massive-financial-hit-from-cyber-attack.

[14] The Register. "M&S cyberattack disruption." 2025. https://www.theregister.com/2025/05/21/ms_cyberattack_disruption/.

[15] ITPro. "Jaguar Land Rover cyber attack financial impact, Cyber Monitoring Centre." Reporting the Cyber Monitoring Centre estimate. 2025. https://www.itpro.com/security/cyber-attacks/jaguar-land-rover-cyber-attack-financial-impact-cyber-monitoring-centre.

[16] BleepingComputer. "Jaguar Land Rover cyberattack cost the company over $220 million." 2025. https://www.bleepingcomputer.com/news/security/jaguar-land-rover-cyberattack-cost-the-company-over-220-million/.

The views in this paper are the author's own and do not represent any employer. Scenarios are hypothetical. This paper is not legal, financial, or compliance advice.