

EXECUTIVE PAPER · DISASTER RECOVERY

A Backup Nobody Has Restored Is a Hope

Most companies pay for backups every month and have never proven they can get the business back from them. Leadership should ask for the proof.

AUTHOR

Chris Watkins

SERVICE

Disaster Recovery

FOR

CEO, CFO · 12 min read

AT A GLANCE

The problem. Backup jobs report success every night, and executives take that as protection. A successful backup job proves that data was copied somewhere. Whether the company can rebuild a working system from that copy, and how long it would take, is a separate question that most organizations have never answered under realistic conditions.

Why it persists. Backup is bought as a product and measured by job completion. Restoring a full system takes people, spare capacity, and a business owner willing to check the result, so it gets postponed. Attackers know this and go after backups first.

The recommendation. Treat every backup as unproven until a scheduled restore test brings the system back intact and a business owner confirms the data. Keep at least one copy isolated from production credentials. Report two numbers per critical system to leadership each quarter: whether the last restore test passed, and how long it took.

The Decision in Front of You

Every company with a server or a cloud account pays for backup. The decision for leadership is whether to keep paying for copies or to start paying for proof.

Proof means restoring real systems on a schedule, timing the work, and having someone outside IT confirm the data is right. Without it, the first real restore happens on the worst day of the year, in front of customers, regulators, and sometimes an attacker who has already been inside the backup system.

The money at stake is large. In a 2024 Sophos study of 2,974 organizations hit by ransomware, victims whose backups were compromised had a median total recovery cost of $3 million. Victims whose backups survived had a median of $375,000 [1].

What's Happening

Confidence runs ahead of results

Veeam's Ransomware Trends Report 2025 surveyed 1,300 organizations, 900 of which had suffered an attack in the prior year. Only 10% of the attacked organizations recovered more than 90% of their data, and 57% recovered less than half [2]. Before they were hit, 69% believed they were prepared [2]. Almost every respondent (98%) had a ransomware playbook, but only 44% of those playbooks covered how and how often backups would be verified [2].

The 2026 edition of Veeam's research, the Data Trust and Resilience Report, drew on more than 900 senior IT, security, and risk leaders. Ninety percent were confident they could recover from a cyber incident. Among ransomware victims whose operations or data were affected, 28% recovered all of it, and the average organization recovered 72% of affected data [3]. Veeam links better outcomes to recovery proven through realistic testing [3]. Veeam sells backup software, so treat these figures as directional.

Restore time is just as overstated. Unitrends' State of Backup and Recovery Report 2025, a survey of more than 3,000 IT professionals, found over 60% believed they could recover from downtime within hours, while only 35% had been able to do so [4]. A quarter of organizations tested disaster recovery once a year or less [4].

Attackers go for the backups first

The same 2024 Sophos study found attackers tried to compromise backups in 94% of ransomware incidents, and succeeded in 57% of those attempts [1]. Exhibit 1 shows what changed when they did.

Exhibit 1. Losing the backups multiplies recovery cost about eightfold

Outcome (2024, median unless noted)	Backups compromised	Backups intact
Data encrypted	85%	52%
Ransom demand	$2.3 million	$1.0 million
Paid the ransom (share of victims)	67%	36%
Total recovery cost, excluding ransom	$3.0 million	$375,000
Fully recovered within one week	26%	46%

Source: Sophos, "The Impact of Compromised Backups on Ransomware Outcomes," survey of 2,974 ransomware victims conducted in early 2024 [1].

Sophos's 2025 survey of 3,400 victims found the share of organizations that recovered data from backups had fallen to its lowest level in six years [5]. The federal guidance is blunt about why. CISA's #StopRansomware Guide notes that many ransomware variants search for reachable backups to delete or encrypt them, and tells organizations to keep offline, encrypted backups and to test their availability and integrity in a disaster recovery scenario [6].

Two recent cases

UniSuper and Google Cloud, May 2024. UniSuper, an Australian pension fund managing more than A$135 billion for over 647,000 members, lost its entire Google Cloud VMware Engine private cloud [7]. Google's review found that operators had left one parameter blank when provisioning the environment in 2023. The system filled in a default one-year term and deleted the private cloud automatically when

that term ran out, without notifying the customer [8]. UniSuper had duplicated the environment across two geographies, and the deletion took out both [7]. Members lost services for an extended period while teams rebuilt hundreds of virtual machines, databases, and applications [7][8]. Recovery depended on backups held with an additional service provider, which the joint statement credits with limiting data loss [7]. The lesson for leadership: replication across regions protects against a regional failure, and only a separately held copy protects against the provider itself.

South Korea's national data center fire, September 2025. A battery fire at the National Information Resources Service data center in Daejeon burned 384 battery packs and took down 96 government systems, disrupting 647 networks [9][10]. Ninety-five of the 96 systems had backups. The exception was G-Drive, a shared storage system used across government, where about 858TB of files, reported as roughly eight years of work, were lost because the system was considered too large to back up [9][10]. About 17% of central government officials were affected [9]. In early October, 115 of the 647 networks had been restored, and officials expected full recovery to take about a month [9][10]. The lesson: a backup program is only as good as its least protected system, and a decision to leave something out is a business decision that leadership should see in writing.

Why the Usual Approach Fails

Most backup programs are measured by the wrong number. The nightly report says jobs completed, which confirms that data reached storage. Whether a running application can be rebuilt from that data, whether the copy is clean, and how many hours the rebuild would take all go unmeasured.

Restores are hard to schedule. A realistic test needs spare compute, an isolated network, an engineer for a day, and a business user to check the records. None of those has a budget line, so the test slips.

Copies share fate with production. Backups that sit on the same network, under the same administrator accounts, in the same cloud tenancy, fail together with the system they protect. UniSuper's two geographies failed together for this reason [7].

Nobody owns the result. When backup belongs to infrastructure and the data belongs to a business unit, each side assumes the other has checked.

The 3-2-1 rule, described in a 2012 US-CERT paper, calls for three copies of important data on two different media types, with one copy stored offsite [11]. That guidance is more than five years old; CISA's current guidance adds offline copies kept out of attackers' reach [6]. NIST SP 800-53 includes control enhancements for testing backups for reliability and integrity, CP-9(1), and for restoring a sample of backup information as part of contingency plan testing, CP-9(2) [12]. NIST SP 800-34 Rev. 1 (2010, still the current federal guide) expects contingency plan tests to include system recovery on an alternate platform from backup media, and for high-impact systems a full recovery and reconstitution to a known state [13]. ISO/IEC 27001:2022 control A.8.13 expects backup copies to be tested regularly against a documented backup policy [14].

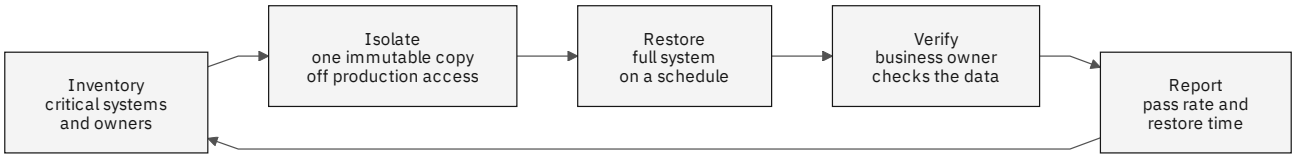
SIDEBAR: THE BACKUPS NOBODY OWNED

In January 2017, an engineer at GitLab accidentally deleted data from the company's primary production database. The team then found its scheduled database dumps had been failing because of a software version mismatch, and the failure alerts had been rejected by the mail server [15]. GitLab restored from a manual snapshot taken about six hours earlier, after roughly 18 hours of copying, and lost database records for at least 5,000 projects [15]. Its postmortem named the root cause plainly: nobody owned the backups, so nobody tested them [15]. The case is older than five years and remains the clearest public account of quiet backup failure.

The Framework: The Restore Proof Loop

The Restore Proof Loop treats a restore test the way finance treats an audit sample. Each critical system is restored on a schedule, the result is checked by someone who knows the data, and the numbers go to leadership.

Exhibit 2. The Restore Proof Loop: a backup counts only after the loop closes



Source: author's framework, drawing on NIST SP 800-34 Rev. 1 [13], NIST SP 800-53 CP-9 [12], and CISA's #StopRansomware Guide [6].

Inventory. List the systems the business cannot run without, and name a business owner for each. Record anything deliberately left out of backup, with the reason and the owner's signature. G-Drive would have appeared on this list [9].

Isolate. Keep at least one copy that production administrators, service accounts, and AI agents cannot alter or delete (an immutable copy), held with a second provider, in locked storage, or offline. Restore tests should draw from this copy at least once a year, because it is the one the company will need after an attack.

Restore. Rebuild the whole system, including the application, its configuration, and its connections, on separate infrastructure. An application depends on a database, an identity service, and a network, and a single restored file tests none of them. Rotate through critical systems so each is restored at least twice a year.

Verify. A business user signs off that the restored records are complete and correct, for example by matching invoice totals or open orders against a known point in time. The engineer's check ends when the server boots; the owner's check covers whether the numbers reconcile.

Report. Each quarter, leadership sees four figures: the share of critical systems with a passed restore in the last six months, the median and longest restore times against the time the business has said it can tolerate, the oldest untested critical system, and the date of the last restore from the isolated copy.

Costs, Risks, and Tradeoffs

Restore testing has real costs, and it is the wrong level of effort for some organizations.

Exhibit 3. Tradeoffs of a scheduled restore program

Area	Cost or risk	Mitigation
Infrastructure	Spare compute and storage to restore into	Use short-lived cloud capacity or a standby environment that already exists for disaster recovery
Staff time	One to several engineer-days per full-system test	Automate restore and verification steps after the first manual run
Business time	Owners must check restored data	Keep checks short: a handful of reconciling totals per system
Test risk	A restore into the wrong network can collide with production	Restore into an isolated network with no route to live systems
Bad news	Early tests will fail and expose gaps	Report failures as findings with owners and dates, the way audit findings are handled
Isolated copy	Immutable or second-provider storage adds cost	Limit it to critical systems and set retention by need
When this is wrong	A small company that runs entirely on SaaS has little to restore itself	Confirm in contracts what the vendor backs up and for how long, export critical data on a schedule, and test that the export opens

Source: author's analysis.

How to Act

Exhibit 4. A one-year restore program

Window	Actions	Owner	Milestone
First 30 days	List critical systems, name a business owner for each, and record every system excluded from backup with a signed reason. Identify which backups production administrators can delete.	CIO or CTO with business unit leaders	Signed inventory; list of exposed backup copies
First 90 days	Create an isolated, immutable copy for each critical system. Run a full restore test of the top three systems into an isolated environment, with owner sign-off.	Infrastructure lead	Three systems restored and verified; restore times recorded
First 90 days	Deliver the first restore report to leadership.	CIO or CTO	Four quarterly figures reported to the CEO and CFO
First 365 days	Restore every critical system at least twice, including at least one restore from the isolated copy. Automate repeatable steps. Map evidence to NIST SP 800-53 CP-9 and ISO/IEC 27001 A.8.13.	Infrastructure lead with risk or internal audit	100% of critical systems with a passed restore in the last six months; audit evidence on file

Source: author's recommendation.

Questions to Ask Your Team

1. When did we last restore our most important system from backup, end to end, and how long did it take?
2. Who outside IT confirmed the restored data was correct?
3. Which systems do we deliberately not back up, and who approved that?
4. If an attacker had our administrator credentials, which backup copies could they delete?
5. Do we hold a copy with a separate provider or in storage that nobody can alter?
6. How long would a full restore of our order or billing system take today, as measured in a test?
7. What failed in our last restore test, and is it fixed?

Closing

A backup that has never been restored is a hope, and the company is already paying for the copies. Spend a modest amount more to restore them on a schedule, have the business confirm the data, keep one copy out of reach of production, and put restore success and restore time in front of the CEO and CFO every quarter.

Sources

[1] Sophos. "The Impact of Compromised Backups on Ransomware Outcomes." Survey of 2,974 organizations, conducted by Vanson Bourne. 2024. https://www.sophos.com/en-us/blog/the-impact-of-compromised-backups-on-ransomware-outcomes.

[2] Veeam. "Veeam Report Finds Close to 70% of Organizations Still Under Cyber-Attack Despite Improved Defenses." Press release, Ransomware Trends Report 2025. 2025. https://www.veeam.com/company/press-release/veeam-report-finds-close-to-70-percent-of-organizations-still-under-cyber-attack-despite-improved-defenses.html.

[3] Veeam. "Veeam Report Reveals a Market-Wide Shift from Recovery Confidence to Proven Data Resilience." Press release, Data Trust and Resilience Report 2026. April 2026. https://www.albawaba.net/business/pr/veeam-report-reveals-market-wide-shift-1625554.

[4] Unitrends. "The State of Backup and Recovery Report 2025." January 2025. https://unitrends.com/resources/the-state-of-backup-and-recovery-report-2025.

[5] Sophos. "The State of Ransomware 2025." 2025. https://www.sophos.com/zh-cn/blog/the-state-of-ransomware-2025.

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

[7] UniSuper and Google Cloud. "A joint statement from UniSuper and Google Cloud." May 8, 2024. https://www.unisuper.com.au/about-us/media-centre/2024/a-joint-statement-from-unisuper-and-google-cloud.

[8] Google Cloud. "Details of Google Cloud GCVE incident." May 24, 2024. https://cloud.google.com/blog/products/infrastructure/details-of-google-cloud-gcve-incident/.

[9] TechRadar. "South Korean government learns it needs a backup the hard way." October 2025. https://www.techradar.com/pro/security/the-south-korean-government-has-learnt-they-need-a-backup-the-hard-way.

[10] DatacenterDynamics. "858TB of government data may be lost for good after South Korea data center fire." 2025. https://www.datacenterdynamics.com/en/news/858tb-of-government-data-may-be-lost-for-good-after-south-korea-data-center-fire.

[11] Ruggiero, P., and Heckathorn, M. A. "Data Backup Options." US-CERT. 2012. https://www.yorkcounty.gov/DocumentCenter/View/11337/Data-Backup-Options.

[12] National Institute of Standards and Technology. "Security and Privacy Controls for Federal Information Systems and Organizations." NIST SP 800-53, control CP-9 and enhancements CP-9(1) and CP-9(2), via STIG Viewer. https://stigviewer.com/controls/800-53/CP-9.

[13] National Institute of Standards and Technology. "Contingency Planning Guide for Federal Information Systems." NIST SP 800-34 Rev. 1, Section 3.5. 2010. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf.

[14] UpGuard. "ISO 27001 Control 8.13: Information Backup Requirements, Implementation, and Audit Guide." Summary of ISO/IEC 27001:2022 Annex A 8.13. https://www.upguard.com/compliance/iso-27001/8-13/.

[15] GitLab. "Postmortem of database outage of January 31." February 10, 2017. https://about.gitlab.com/blog/postmortem-of-database-outage-of-january-31/.

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.