Your Backups Are Lying to You

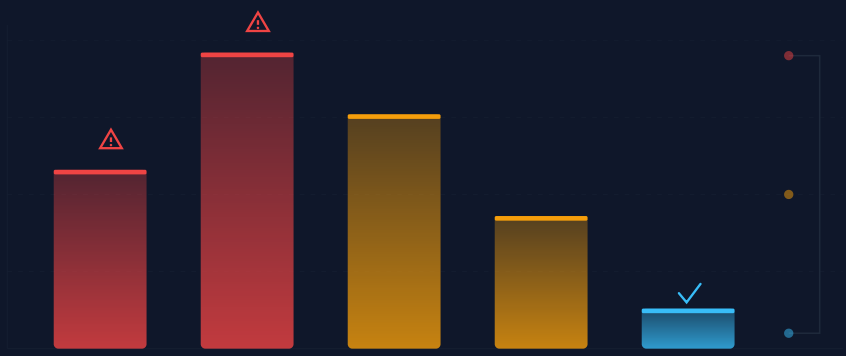
A plain-language guide for IT directors, CFOs, and business owners

What to ask your team this month. What auditors want to see. What it costs if you guess wrong.

Rediacc | 2026

The Bill Most Companies Cannot Pay

58% of backups fail when someone tries to use them



Veeam surveyed 1,200 companies and confirmed the **58% restore-failure rate** above (Veeam 2024). Only 13% of those companies could bring back everything during a real disaster test.

Now add the attacker. Ransomware crews target the backups in 96% of attacks, and they succeed 76% of the time (Veeam 2024).

When the backups are wrecked, the bill jumps eight times. Sophos 2024 puts recovery at $3 million with broken backups, against $375,000 with working ones.

Like having a fire extinguisher you have never checked. You find out it is empty when the fire starts.

Ask your IT team: when did we last bring back a real system from backup?

One Third Never Test. The Rest Find Failures.

"Backup completed successfully" tells you nothing

About one third of businesses never test their backups (Computer Weekly). Of those that do test tape backups, 77% find failures (Pivotal IT).

The Veeam 2025 Ransomware Trends Report found that only 44% of ransomware playbooks even include a step to check the backup. Only 37% boot the backup in a safe area before bringing it back.

Downtime makes the math worse. The ITIC 2024 survey of 1,000 firms found mid and large companies routinely lose $1 to 5 million per hour when systems are down.

Average ransomware recovery takes 3.4 weeks and costs $2.73 million, before any ransom (Sophos 2024).

Like cooking the meal you have been freezing for emergencies, once a month, so you know it still tastes right.

Ask your IT team: do we have a test that actually starts up the backup?

When "Backup Completed Successfully" Was a Lie

Three companies. Three nights nobody slept.

An engineer at GitLab deleted the wrong database in 2017. They had five backup systems. Four of them were not actually working.

They lost six hours of customer work and live-streamed the recovery to 5,000 viewers.

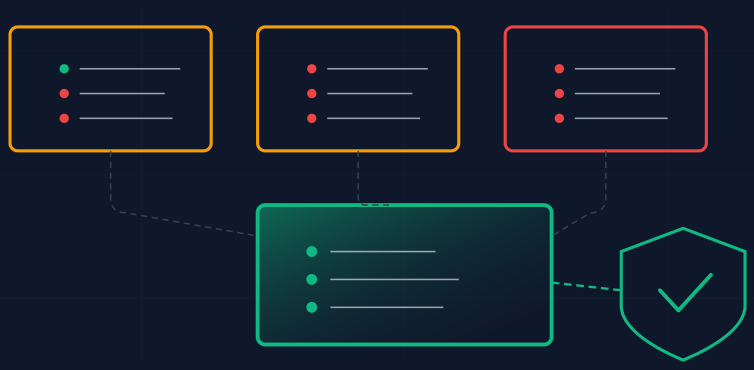
Maersk's shipping company was hit by ransomware in 2017 and lost almost everything. They found one accidentally offline domain controller in Ghana that saved the company. That is not a backup strategy.

Travelex's currency exchange paid the ransom in 2019 because their backups had been incomplete for months. They did not know until they needed them. The company went bankrupt by August 2020, costing 1,300 jobs.

The common thread: each one believed the backups worked. None had checked. A backup you have not tested is not a backup. It is a hope.

What Your Backup Vendor Sells You vs. What You Get

Most vendors market depth they do not deliver



Vendor	Tests the backup actually boots?	Notes
Veeam (SureBackup feature)	Yes, but 3 servers at a time	Enterprise tier only
Rubrik	Manual, via scripts	Requires very large deals
AWS Backup	Restore only, since Nov 2023	Does not check the system works
Azure Backup	No automated check [^1]	Microsoft says do it by hand
Datto	Yes, screenshot of boot [^2]	Only sold via partners

[^1]: Microsoft's own guidance tells Azure customers to script their own tests.
[^2]: Datto has led the small and mid-size market with screenshot tests since 2011.

Veeam's testing feature (limited to 3 servers at a time) is the deepest of the big names. It still leaves most of the estate unchecked.

Ask your vendor: how do you prove every backup actually starts up?

What Your Auditor Now Demands

The rule has changed from "do you back up?" to "prove it works"

The HIPAA rule that covers healthcare records (45 CFR 164.308(a)(7)) requires you to test the backup. Penalties reach $2.13 million per violation category per year.

The GDPR rule that requires you to be able to restore data after an incident (Article 32) carries fines up to 4% of global sales. Albany ENT paid $1M. Enzo Biochem settled for $4.5M (HHS OCR settlements 2023-24).

Ask your compliance officer: can we hand the auditor a report showing every backup was tested last quarter?

What Your Insurance Company Now Demands

Say "yes, we test" when you do not, and your claim is denied

ISO 27001 is the global rule for info security. Its 2022 update requires regular backup tests.

PCI-DSS 4.0 covers card payments. It now requires a yearly disaster-recovery test.

Cyber insurance has become the enforcer. About **41% of cyber insurance claims are denied** on first try (Marsh McLennan 2024). Bad backup habits are a top reason.

Tell the insurer you test your backups, then fail to test, then get hacked, and the claim is denied. Get the answer in writing before renewal.

Firms that pair multi-factor login, modern antivirus, and tested locked backups can cut premiums by **20 to 50%** (Marsh McLennan 2024). At-Bay 2024 found tested backups cut ransomware claim cost by 41%.

Call your insurance broker this month: ask what you need to show at renewal.

How Continuous Testing Works

Every backup gets a green light, every day

Rediacc does the testing for you. Every backup is started up in a safe area and checked: does the operating system load? Do the apps start? Does the database open?

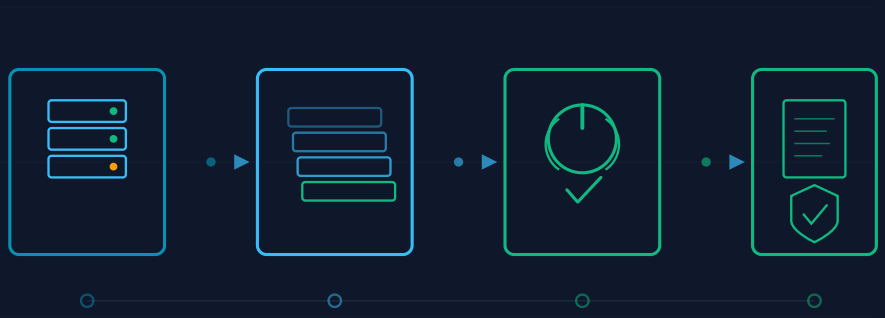
You get a green light on every backup, every day. Or you get an alert before the attacker does.

Like test-driving the spare car every Monday, instead of finding out it will not start the morning you need it.

Ask your IT team: which of our systems get an actual boot test, not just a file copy check?

What "Tested Backup" Actually Means

Capture, save, boot, report



Capture. A backup copy is taken in under a second.

Save. Minute-by-minute copies are kept without filling the disk.

Boot. Each saved copy is started up in a safe area, and the apps are checked.

Report. Every test gets a timestamp and a pass-or-fail, written down for the auditor.

The boot step is the one that matters. It catches the failures that file-copy checks miss.

Like test-driving the spare car every Monday, instead of finding out it will not start the morning you need it.

The Money Question

Spend $50K to $200K a year, or pay seven figures when it goes wrong

The average ransom payment hit $2 million in 2024 (Sophos 2024). That is a 500% jump from $400,000 the year before. The recovery bill comes on top, often in the millions.

Rediacc estimates a tested-backup program costs about $50,000 to $200,000 a year. That is for a firm with 50 to 500 servers. It works out to under 5% of one bad incident.

Scenario	Yearly Spend	Worst Case
Tested backups	$50K to $200K	Routine recovery
Untested backups	Whatever you spend today	Multi-million ransom plus recovery

Ask your CFO: what is the budget line for "ransomware did not happen this year"?

Find out if your backups would survive.

Rediacc tests every backup by starting it up. You see a green light, or you see the failure before the attacker does.

Continuous boot-and-verify testing. Minute-by-minute backup copies. One report your auditor and your insurance broker can both read.

rediacc.com

Rediacc | Tested backups. Verified recovery in minutes.