Your Backups Will Be Attacked. Will They Survive?

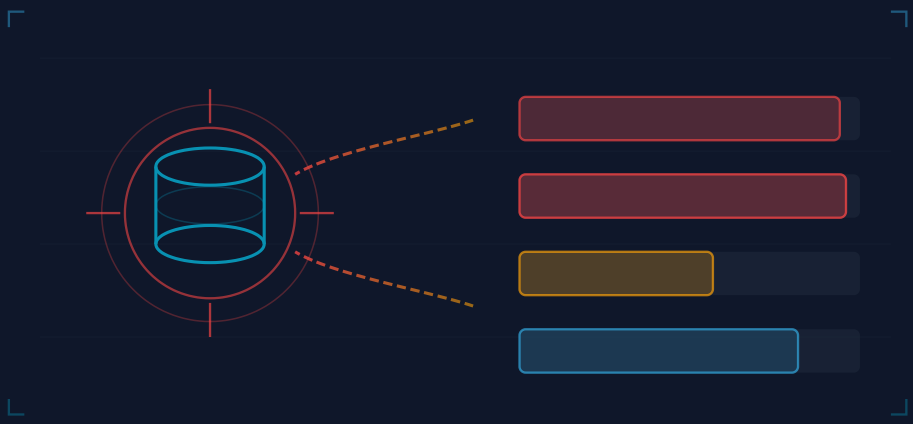
A plain-language guide for IT directors, CFOs, and business owners

What to ask your team this month. Why your insurer cares. What it costs if you guess wrong.

Rediacc | 2026

The Bill After an Attack

Recovery now costs more than most companies hold in cash



The average company hit by ransomware spent $1.53M to recover in 2025 (Sophos).

That figure does not include the ransom itself. Add the ransom and IBM puts the full cost at **$5.08M** per incident.

In the US the average climbs to $10.22M (IBM 2025).

Paying the ransom is not a fix. Only 7% of companies that paid got all their data back (Hiscox).

84% of paying victims still lost data (Sophos 2024). And 80% of companies that paid were attacked again within a year (Halcyon 2024).

That is why **64%** of companies now refuse to pay (Verizon DBIR 2025), up from half just three years ago.

The math on paying is broken. The math on preventing the damage is not.

Ask your IT team: what would a one-week outage cost us in lost sales?

The Burglar Goes for the Spare Keys First

Attackers try to destroy your backups in 94% of attacks

The single most important fact in this deck: in **94% of ransomware attacks**, the attackers try to wreck the backups before they encrypt anything (Sophos 2024). They succeed 57% of the time.

Think of a burglar who finds the spare keys and destroys them before robbing the house. Even after they leave, you cannot get back in.

When the backups are destroyed, the bill jumps. Recovery costs go from $375K to $3M, an **8x increase** (Sophos 2024).

Recovery time stretches from under a week to over a month.

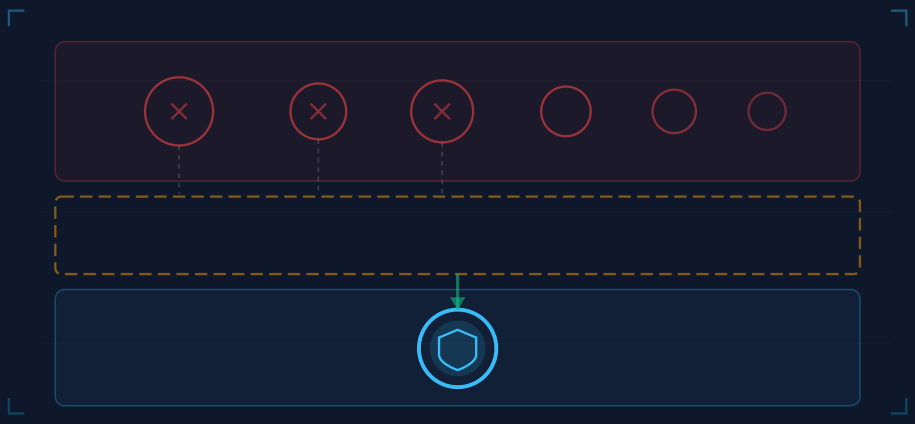
And 67% of victims with broken backups pay the ransom, versus 36% with clean backups.

Smaller companies are not safe. 88% of ransomware breaches hit small and mid-sized businesses (Verizon DBIR 2025), the ones priced out of tools built for the biggest companies.

Ask your IT team: if a hacker stole our top admin password tonight, could they delete our backups?

Added-On Locks vs. Built-In Locks

Why most "immutable backup" claims fail under attack



Most backup vendors say their backups are "locked," meaning they can't be changed or deleted. The fine print is that the lock is added on top of regular storage.

A bike lock can be cut. A bike with no chain wheel has nothing to cut.

Veeam, the biggest name in backup, uses a Linux setting called the "immutable flag" to lock files.

Veeam itself recommends putting the backup server in a locked room with cameras. That recommendation tells you something: software alone is not enough.

Other vendors lock the files but not the storage. Some only sell to companies with **250TB** or more of data, with deals over **$200K** a year (public vendor pricing 2024).

The pattern: every option locks the backup files but not the storage they sit on. An attacker with the top admin password can usually find a way past.

Ask your vendor: can the top admin password defeat your locks on the backup server? Get the answer in writing.

How a Locked-Storage Approach Works

The Polaroid that can't be edited

Rediacc builds backups on btrfs (an open-source storage system built into Linux). The storage layer itself makes each backup copy locked the moment it is created.

Picture a Polaroid of your filing cabinet taken at 9 a.m. every day. The photo can't be edited.

If a thief breaks in at noon, you still have a clean photo from 9 a.m. to rebuild from.

The storage layer also keeps a fingerprint of every file. A built-in command checks the fingerprints and flags any file that has been changed or quietly broken.

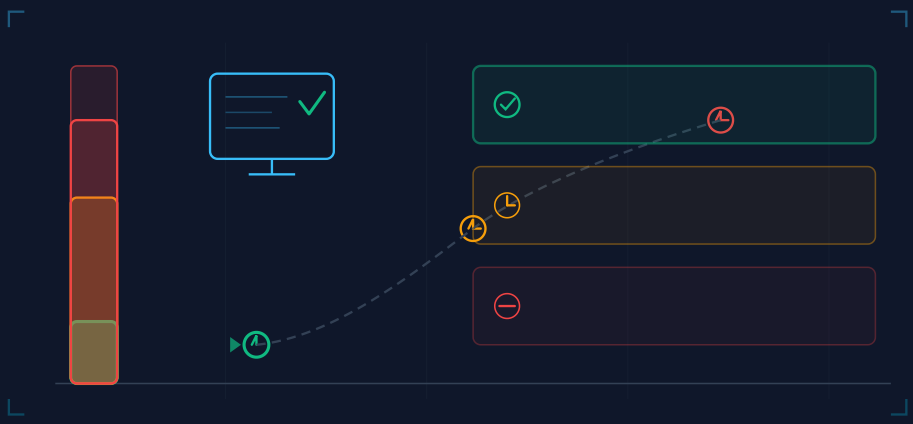
This matters because **31%** of recovery attempts fail (At-Bay), often because nobody noticed the backup was already broken.

Each backup copy gets a date, a time, and a fingerprint. The records satisfy both auditors and your insurance company without extra work.

What this gives you: backup copies that an attacker with the master password still cannot change or delete.

Recovery Speed: Minutes, Not a Month

Two stores after a power cut. One stays dark. One keeps selling.



The average ransomware outage lasts **24 days** at about **$88,000 per hour** in lost business (Veeam). A single attack can cost over $50M in downtime alone.

Even tools that advertise "instant recovery" do not deliver. Veeam's instant recovery runs your servers from backup at slow speed.

A full restore of a 5TB server still takes 4 to 6 hours.

Picture two stores hit by a power cut. One is dark for a month, the other flips the breaker and keeps selling.

The first copies every file back. The second just points at the saved copy and runs.

Rediacc does the second one. The system points at the saved version and runs.

You can also test-drive the spare car every Monday. Boot the backup, check it works, before you ever need it.

"We think our backups work" becomes "we know they do."

Ask your IT team: when did we last fully test a restore?

What Your Auditor and Insurer Now Demand

Locked backups are no longer optional

Four rules have changed the math on backup spending in the last two years.

SEC 8-K is the rule that makes public companies report a hack within 4 business days. Fines can reach **$25M**.

DORA is the EU rule for financial firms, in force January 2025. Fines can reach 2% of global sales.

NIS2 is the EU rule for 18 key industries. Fines can reach $10M or 2% of sales.

Most cyber insurers now ask for locked backups: **73 to 75%** of them (AI Readiness Lab 2025).

The insurer asks: can a hacker with your top admin password delete your backups? Say no when the answer is yes, and your claim is denied.

Proven locked backups cut your premium 20 to 50% (Marsh 2024). Reports come straight from the backup system, like a credit card statement.

Call your insurance broker this month: ask what they need to see at renewal.

Why "Just Use AWS Backup" Is Not Enough

Amazon protects Amazon. Your business runs on more than that.

The three big cloud providers all sell locked backup for their own services. AWS protects AWS.

Microsoft Azure protects Azure. Google protects Google.

None of them protect the others. None of them protect your own servers.

73% of companies now run on a mix of cloud providers and their own buildings (Flexera 2024). Cloud-only locked backup covers only part of what matters.

Recovery from cloud backup also runs at network speed. The data has to travel back to where your business runs.

For a large company that is hours of waiting while every minute costs money. The fix has to cover all of it: Amazon, Microsoft, Google, and your own servers.

Ask your IT team: which of our systems are not covered today?

The Money Question

$375K vs. $3M. The eight times multiplier.

The numbers from Sophos draw a sharp line between a working backup and a broken one.

Scenario	Recovery Cost	Time Down	Pays Ransom
Backups broken	**$3M**	Over 1 month	67%
Backups working	**$375K**	Under 1 week	36%

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

Find out if your backups would survive.

Rediacc locks the storage itself. An attacker with the top admin password still cannot reach the backups.

94% of ransomware attacks target backups. 57% succeed.

A working backup costs $375K to recover from. A broken one costs $3M.

rediacc.com

Rediacc | Locked backups. Verified recovery in minutes.