SCALITY
ARTESCA

The Cost of Downtime

How outages and slow recovery hit small and mid-size businesses, what actually drives the cost, and how to estimate your own exposure.

An outage costs you for every hour you are offline, multiplied by what an hour is worth.

This brief is written for small and mid-size businesses. At its core the cost of an outage is simple: how long the business is offline, multiplied by what an hour of that business is worth.

What counts as an hour offline depends on how a business operates. A back-office team loses the hours its people cannot work. A shop or an online seller loses the hours it cannot trade, and only during the hours it would have been trading. The first number to pin down is how many hours of a normal day would actually be lost: eight, twelve, or a full twenty-four.

What an hour is worth is more than lost sales. It includes the staff who are paid while they wait, the overtime and outside help to put things back, and the orders that never come back later. Together those turn a single down hour into a number worth acting on.

Mid-size businesses feel this more sharply than the giants. They run on the same always-on systems, but with smaller teams, thinner redundancy, and less cash to absorb a bad month. An outage a large enterprise can shrug off can put a mid-size company under real strain.

And the bill does not stop when systems return. Most organizations never recover all of their data after a serious incident. Whatever does not come back, customer records, work that took weeks to produce, history that cannot be rebuilt, carries its own cost. This brief covers both halves: what an outage costs while the business is down, and what it costs in data that never returns.

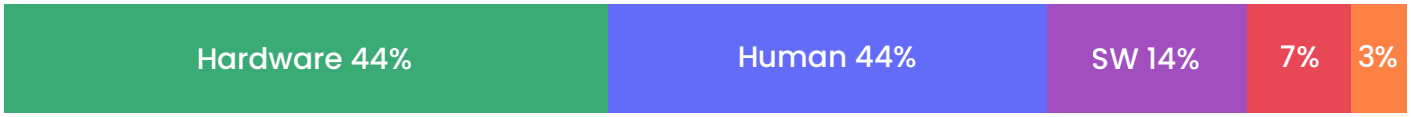
The encouraging part is that most of the cost is controllable. The hours offline and the data that survives are both decided by one thing: where the backups live and how fast they come back. That is the lever this brief focuses on.

HOW THIS BRIEF CAME TOGETHER

The figures here come from independent industry research published between 2024 and 2026, combined with close to two decades of Scality experience in storage built for backup. From that we built a deliberately simple model. The studies and links are listed in the annex.

Hardware and people cause more outages than hackers do.

Most events that force a restore are ordinary. A drive fails, someone deletes the wrong volume, an update corrupts a database. Across studies the split is roughly consistent.



44% HARDWARE FAILURE

Failed drives, controllers, power and cooling. Still the single most common cause of data loss.

32% HUMAN ERROR

Accidental deletion, misconfiguration, a skipped step. People remain a leading cause in every study.

14% SOFTWARE AND CORRUPTION

Bad updates, failed migrations, application or database corruption that spreads before anyone notices.

7% CYBERATTACK AND RANSOMWARE

The smallest share of events, and a different kind of problem from the rest.

3% NATURAL DISASTER

Fire, flood, physical site loss. Rare, but it takes everything in one location at once.

Almost all of these are accidents. Ransomware is the exception. It is deliberate, built to cost money and do damage, and it goes straight for the backup so that recovery is as hard as possible. The smallest share of incidents, and the one designed to be the hardest to come back from.

How do you calculate the cost of an outage?

It comes down to two numbers multiplied together: how long the business is offline, and what an hour offline is worth. Three parameters set those two numbers.

01 Hours of exposure per day

How much of a normal day is actually lost. A nine-to-five office loses around eight hours. A 24/7 operation loses all twenty-four. An online business loses only the hours it would have been trading.

02 What an hour is worth

Lost revenue for the hour, the staff who are paid while they wait, and the labour and overtime to recover. Together they make up the hourly cost.

03 How long recovery takes

The more data there is to restore, the longer it takes, and the speed depends on the backup target. This is what turns a bad hour into a bad fortnight

THE FORMULA

Outage cost = hourly cost × hours offline

hourly cost = lost revenue + idled staff + recovery labour
hours offline = hours of exposure per day × days to recover

A per-hour figure says little on its own. Multiplied across a recovery that can run for days, it becomes the real number. The next page works a single example through end to end. The companion calculator runs the same formula on your own figures.

How do you calculate the cost of an outage?

300

employees

€9,000

per hour offline

500 TB

data protected

Picture a mid-size European company: a regional distributor with around 300 employees that takes orders, runs a warehouse, and supports customers through the working day. No attacker involved, just a bad week.

A primary storage system fails and corrupts the data on it. The only clean copy is the backup, so the business has to restore 500 TB before it can operate normally again. Orders stall, the warehouse cannot ship, and support cannot pull customer records. On a conventional backup target, restoring that much data takes around six working days.

Across those days the business loses roughly eight productive hours a day. At about €9,000 an hour, the downtime alone comes to around €432,000, from a routine hardware failure, before anyone mentions a cyberattack.

€432K

The downtime cost of one outage, on conventional backup

€9,000/hour × 8 hours/day × 6 days · no data loss assumed

The data you do not get back.

In the example the backups held and the data came back. That is the good case. When the backup itself fails or is targeted, recovery is rarely complete, and that is the second half of the cost.

Average across organizations hit by a serious incident. Veeam, 2024.

On average **43% of the data affected in a serious incident is not recovered.** That gap is not abstract. It is customer records that can no longer be billed or served, work that took weeks to produce, contracts and history that cannot be rebuilt from anywhere else. Whatever that data is worth to the business, it adds to the downtime cost rather than replacing it.

This is the half that matters most when the cause is malicious. Ransomware goes after the backup precisely so the clean copy is gone when it is needed, which is why so much data is lost in an attack and why recovery drags on for weeks. **Unlike downtime, this half does not come back at any price.**

The answer is immutable storage.

A backup that cannot be encrypted, altered, or deleted survives every cause in this brief, and a target built for fast restore brings it back in a day, not weeks. **ARTESCA** is that storage: secure, built for backup, and simple to run.

Secure

Immutable storage with S3 Object Lock and CORE5 cyber resilience. A backup cannot be encrypted or deleted, even by a compromised admin, so the recovery gap goes to zero.

Built for backup

Fast restores at scale, validated with Veeam, Commvault, Rubrik, Cohesity and the rest of the major backup stack. Scales from 20 TB to 8.5 PB

Simple

Set up in minutes, run by a normal IT team, no deep storage or OS expertise required. Backed by the $100,000 ARTESCA Cyber Guarantee.

CORE5 · FIVE LEVELS OF CYBER RESILIENCE

Level 1 API	S3 Object Lock makes every backup immutable the moment it is written. Ransomware that mimics application commands cannot encrypt or delete it.
Level 2 Data	Encryption in flight and at rest, multi-factor authentication, and locked-down access stop exfiltration and unauthorized changes on the network.
Level 3 Storage	Erasure coding spreads data across the cluster so an attacker reaching the disks cannot read or rebuild anything useful.
Level 4 Geographic	Replication across sites removes the single-location risk from fire, flood, or physical breach.
Level 4 Architecture	A hardened operating system with no root access and no way to lift the lock, so the system itself cannot be turned against the data.

The same outage, with ARTESCA.

Run the example again with an immutable, fast-restore target. Same company, same 500 TB to restore. Only the storage changes.

CONVENTIONAL BACKUP

DOWNTIME COST

€432K

Six days offline before the business runs normally again.

DOWNTIME COST

€72K

About one day offline, restored from an immutable copy.

VALUE OF DATA LOST

?

Unknown. If the backup is hit, the data never comes back at any price.

DATALOS

None

The copy stays complete, even when the cause is malicious.

The ARTESCA Cyber Guarantee. If ransomware defeats the immutability of a covered ARTESCA deployment and the data cannot be recovered, Scality pays $100,000. Industry-first, on every commercial license, even at 50 TB, subject to the program terms.

Sources and further reading.

Every figure in this brief comes from independent, published research. The studies behind each claim are listed below.

Uptime Institute	Annual Outage Analysis 2024. Cost and frequency of significant outages; 54% of serious outages exceed €100,000.
ITIC	2024 Hourly Cost of Downtime Survey, 1,000+ firms. Hourly cost of downtime by organization size and sector.
Coveware	Quarterly Ransomware Report. Average downtime duration after a ransomware incident, around 21 days.
Veeam	2024 Ransomware Trends Report (43% of affected data unrecoverable) and 2025 Ransomware Trends (backups targeted in 89% of attacks). Data Protection Trends 2024 for recovery-readiness figures.
Sophos	State of Ransomware 2024 and 2025. Recovery cost with and without compromised backups.
Cause-of-loss data	Hardware, human error, software, cyber and disaster shares synthesized from 2024 data-loss and data-center outage analyses; figures vary by source and are presented as indicative
ARTESCA	Product capabilities, CORE5 cyber resilience, and the $100,000 Cyber Guarantee. Scality, artesca.scality.com.