
FROM THE MEHRUTHERM BLOG · MANAGED IT

If You've Never Tested Your Backup, You Don't Have One

A single external drive or 'it's all in the cloud' is not a backup plan. Here is what a backup you can actually restore looks like, in plain English.

Himanshu Mehru · Founder, Mehrutherm

June 25, 2026

Here is an uncomfortable question. If everything disappeared tomorrow, the files, the records, the photos of jobs, the spreadsheet the whole office runs on, how quickly could you get it all back?

Most owners answer with a confident "we're covered." Then the day actually comes, a drive dies, a laptop is stolen, ransomware locks everything up, and they discover the backup in the desk drawer has not run since last spring, or the cloud folder faithfully copied the damaged files right over the good ones. The plan they were sure they had turns out to have been an assumption.

A backup is one of those things that is either there when you need it or worthless. There is very little in between.

A copy is not the same as a backup

The most common mistake is treating a single copy as safety. A folder that automatically syncs to the cloud feels like protection, and for a dropped laptop it is. But sync is a mirror, not a vault. If a file gets deleted, corrupted, or encrypted by ransomware, the sync does its job perfectly and copies the broken version everywhere. Now both copies are bad.

One copy in one place, however convenient, is exposed to whatever happens to that place. Real protection comes from having more than one copy, in more than one kind of place.

The simple rule that actually holds up

You do not need anything complicated. A backup you can trust follows a rule of thumb that has protected organizations for years:

- Keep **more than one copy** of anything you cannot afford to lose.
- Keep those copies on **more than one kind of storage**, not all on the same machine or the same drive.
- Keep **at least one copy off-site**, somewhere a fire, a theft, or a flood at your office cannot reach it.

That is the whole idea. More than one copy, more than one place, one of them somewhere else.

KEY TAKEAWAYS

- A folder that **syncs** protects against a lost device, not against deleted, corrupted, or encrypted files.
- Keep **more than one copy**, on **more than one kind of storage**, with **one copy off-site**.
- A backup you have **never restored** is a hope, not a plan.
- Ransomware is far less frightening when you can simply **roll back** to yesterday.

The step almost everyone skips

Here is the part that separates a real backup from a comforting story: testing the restore.

A backup that has never been restored is an unproven assumption. The drive might be failing silently. The job might have quietly stopped running months ago. The files might be there but unusable. You do not want to discover any of that on the worst day of your business year, with customers waiting and the clock running.

The fix is not glamorous. Every so often, you actually restore something and confirm it comes back clean. That single habit turns "we think we're backed up" into "we know we can recover," and it is the difference between a bad afternoon and a closed business.

RANSOMWARE COUNTS ON YOU NOT HAVING THIS

The whole business model of ransomware is that getting your files back is worth paying for. A tested, separate backup quietly removes their leverage: instead of a ransom and days of downtime, recovery becomes a roll-back to yesterday. The attack still happened, but it stopped being a catastrophe.

What this looks like when someone is watching it

Done right, none of this is something you should have to remember. The copies are made on a schedule, kept in more than one place, and a restore is tested now and then to prove it all works, without you having to think about it.

That is exactly the kind of quiet, ongoing work [managed IT](#) is built for. For the businesses and towns we look after, the backups run, get checked, and are kept somewhere safe, so that the day something goes wrong is an inconvenience instead of a disaster. For towns especially, that resilience is also part of [what insurers now expect](#), and it sits right alongside the [other security basics](#) worth having.

MEHRUTHERM · CRESTON, WA

Not sure your backups would actually save you? Get in touch and we'll check whether they would hold up, and set up a recovery plan you can count on.

mehrutherm.com/quote