FREE GUIDE

The First 5 Backup Mistakes Small Businesses Make

The five ways backups quietly fail, and the plain-English fix for each one.

Almost every small business believes it has backups. Far fewer could actually recover tomorrow morning. The difference is rarely the technology. It's a handful of quiet mistakes that don't announce themselves until the worst possible day. Here are the five most common ones, in the order worth fixing them.

A free guide from Sylvan Assurance — plain-English security, without us ever seeing your data.

Mistake 1: The backup can be reached by the same problem it's protecting you from

What it looks like

Your backup drive is plugged into the computer it backs up. Or the backup lives in the same account, behind the same password, as everything else. It works perfectly, right up until software that locks your files for ransom finds the backup too, and locks that as well.

The fix

Keep at least one copy somewhere a problem with your main systems can't reach: a separate cloud backup with its own login (and two-step login turned on), or a drive that isn't left connected. The test question is simple: "if everything I can touch from this computer got locked tonight, is there still a copy somewhere else?"

Mistake 2: Nobody has ever actually restored anything

What it looks like

The backup runs. The little icon is green. And no one has ever tried to bring a file back from it. An untested backup is a hope, not a plan. Businesses routinely discover theirs was misconfigured, incomplete, or quietly broken, at the exact moment they need it.

The fix

Once a quarter, pick one file and restore it. Five minutes. If that feels easy, once a year try restoring a whole folder and note how long it takes. That number tells you what a genuinely bad day would look like.

Mistake 3: Backing up the computer, but not the business

What it looks like

The office desktop is backed up faithfully, while the real business lives in a bookkeeping app, a cloud drive, an email account, and one laptop that travels. The thing you'd actually cry over losing isn't in the backup at all.

The fix

Make a short list titled "what would hurt if it vanished": customer records, the books, contracts, email, photos of the work you've done. Then check each one: where does it live, and is that place backed up? Most cloud apps keep your data available, but "available" is not the same as "recoverable if it's deleted or corrupted". Many businesses add a backup of the cloud data itself.

Mistake 4: One copy, in one place

What it looks like

There is a backup: exactly one, sitting on a drive in the same room as the computer it protects. A fire, a flood, or a burglary takes the original and the backup in the same afternoon.

The fix

The old rule of thumb still holds, in plain English: keep two copies of anything important, and keep one of them somewhere else. For most small businesses that's one local copy (fast to restore) plus one cloud copy (survives anything that happens to the building).

Mistake 5: The backup belongs to nobody

What it looks like

Someone set it up years ago and moved on. For a while it emailed errors to an inbox no one checks. It stopped in March, and stayed stopped, because keeping an eye on it was never anyone's job.

The fix

Give the backup an owner by name. In a tiny business, that's you, written down. The job is five minutes a month: confirm the last backup ran, confirm the error alerts go somewhere a human looks, and do the quarterly one-file restore from Mistake 2. A backup with an owner fails loudly; a backup without one fails silently.

The honest summary

None of this requires a security background or a big budget. One copy a problem can't reach, a restore you've tried, coverage that matches where the business lives, two copies with one elsewhere, and a named owner. Do those five and you're ahead of most small businesses, and far better positioned against the most expensive bad day there is.

Where to go from here

The free SMB Security Assessment shows you where your business stands in about five minutes, and it runs entirely in your browser, so we never see your answers.

When you're ready to turn that snapshot into a plan with the templates to carry it out, the Full Edition lays it all out: one-time purchase, 30-day money-back guarantee.

Take the free assessment: sylvanassurance.com/free/smb-security/

See the Full Edition: sylvanassurance.com/smb-security-assessment.html

Scan for the free assessment that goes with this guide.
sylvanassurance.com/go/free-smb-security-assessment