BUSINESS BACKUP

How To Back Up A Small Business Without Cloud Lock-In

Plain-English how-to. ~3 hours setup. Resilient backup + ransomware recovery for any small team.

Most small businesses discover their backup strategy was inadequate at the exact moment they need it — when ransomware hits, when a cloud provider locks the account, when a laptop is stolen. By then it's too late.

The good news: small business backup has gotten cheap and reliable. Built right, it costs about $20-50/month, survives ransomware, recovers within hours, and doesn't lock you into any single vendor. The pattern is called 3-2-1 — three copies, two media, one offsite — and it's been the gold standard for decades because it works.

By the end of this guide your business will have a verified 3-2-1 backup covering every critical system, with documented recovery procedures and a quarterly test that catches problems before they matter.

Quick snapshot

What you'll learn	Build a vendor-independent 3-2-1 backup with local NAS, encrypted cloud, and offsite copies.
Skill level	Intermediate · Owner / IT lead
Time required	3 hours initial setup; 30 min/quarter to test
What you'll need	$300-500 for NAS, ~$10-30/month cloud, list of systems to back up
Risk if you skip this	Ransomware = closed business. ~60% of SMBs hit by ransomware fail within 6 months.
PDF kit	■ Download at the bottom of this page

Why this matters

Ransomware specifically targets small business backups. Modern ransomware finds and encrypts attached storage and connected cloud drives before encrypting the primary systems — leaving the victim with nothing.

The 3-2-1 rule defeats this: three copies (production + 2 backups), two different media (local + cloud), one offsite. Even if ransomware kills two copies, one survives.

Vendor independence matters too. If your only backup is in one SaaS provider, you're dependent on that provider not locking your account, going bankrupt, or being breached themselves. Diversification protects against single-vendor failure.

Before you start

Inventory what needs to be backed up: file shares, email (yes, M365/Google Workspace too), accounting data (QuickBooks, Xero), CRM exports, source code, vendor documents.

Decide on RTO (Recovery Time Objective) and RPO (Recovery Point Objective): how long can the business be down, and how much data can you afford to lose? Answers drive the design.

Budget: a basic 3-2-1 for a 10-person business is $300-500 in hardware, $10-30/month in cloud. Time investment is ~3 hours setup, ~30 min/quarter ongoing.

Step 1 — Copy 1: Production data (already done)

Your live systems — laptops, file servers, M365/Google Workspace, QuickBooks Online — these are 'copy 1.' Don't conflate them with backup; they're the source.

Verify they have basic redundancy (RAID, cloud replication). This doesn't replace backups but reduces single-disk failure risk.

Step 2 — Copy 2: Local NAS (fast restore)

Buy a NAS: Synology DS923+ or QNAP TS-464 around $500 plus drives. Set it up in RAID 5 or RAID 6 (~3-4 drives).

Configure it as an SMB share. Use built-in backup tools (Synology Active Backup, QNAP HBS) to pull daily backups from laptops, servers, and SaaS (M365/Google Workspace).

Step 3 — Copy 3: Offsite encrypted cloud

Use a cloud-backup service designed for businesses: **Backblaze B2** ($6/TB/month), **Wasabi** ($7/TB/month), or **Cloudflare R2**. Encrypt files locally before upload with a key only you hold.

Use a backup tool like **Duplicati** (free, open-source) or **Synology HyperBackup** to push encrypted backups to the cloud from your NAS.

Step 4 — Air-gap your backups

Ransomware that infects the network can encrypt the NAS if it's reachable. Either: use immutable / WORM (Write Once Read Many) storage features on the NAS, OR rotate a USB drive monthly as a true offline copy.

The offline copy is the last line of defense. Even if ransomware kills your live and NAS backups, the USB drive in your safe is untouched.

Step 5 — Back up cloud-only data (M365 / Google Workspace)

Many businesses assume 'it's in the cloud, it's backed up.' Wrong. M365 and Google Workspace have limited recovery windows (30-90 days). After that, deleted data is gone.

Use **Synology Active Backup for Microsoft 365** or **Spanning** or **SkyKick** to pull SaaS data to your local backup. Same approach for QuickBooks Online, HubSpot, etc.

Step 6 — Document the recovery procedure

Write a one-page runbook: 'If a laptop is encrypted by ransomware, do X. If the server is wiped, do Y. If we're locked out of M365, do Z.' Specify time estimates and who owns each step.

Store the runbook somewhere not on the systems being backed up (print it, save in password manager, put in fireproof safe). It's worthless if it disappears with the data.

Step 7 — Test quarterly with a real restore

Every quarter, restore one random file from each backup tier (NAS, cloud, USB) and verify it opens and is current. Most 'we have backups' businesses have never tested restore — and the actual restore fails.

Once a year, run a full system restore simulation: pretend a key laptop is gone and restore from backups end to end. Time the process. Update the runbook with what you learn.

Step 8 — Verify ransomware survivability

Confirm that the credentials used by your backup software CANNOT modify or delete backups (use append-only roles, immutable buckets, separate accounts). This is what makes ransomware not eat the backups.

On Backblaze B2 / Wasabi: enable Object Lock with a 30-day retention. Even if attackers have your account credentials, they cannot delete the data.

PRO TIP

Untested Backups Don't Exist.

Every 'we had backups' ransomware story ends with 'and they didn't restore.'

Quarterly file-level restore test catches 90% of problems.

Annual full-restore drill catches the rest.

Object Lock / immutable storage is the ransomware insurance you actually need.

If you want to go further: power-user upgrades

Power-user upgrade #1 — Add a second cloud provider

Backblaze + Wasabi (or B2 + R2) — diversifies vendor risk. If one is breached or locks accounts, the other survives.

Trade-off: ~2x cloud cost.

Power-user upgrade #2 — Implement Veeam Backup & Replication

Enterprise-grade tooling for SMBs. Veeam Community edition is free for up to 10 workloads.

Trade-off: setup complexity.

Power-user upgrade #3 — Set up bare-metal recovery images

Veeam Agent or Macrium Reflect creates full-disk images. Restore replacement hardware in hours, not days.

Trade-off: requires extra storage per image.

Power-user upgrade #4 — Implement WORM compliance for regulated data

If you handle HIPAA, PCI, or financial data, immutable backups are often required, not optional.

Trade-off: storage overhead.

Power-user upgrade #5 — Encrypt with KMS

Use a Key Management Service for backup encryption keys. Rotates keys without re-encrypting all data.

Trade-off: KMS subscription.

Power-user upgrade #6 — Document escrow

If your business is sold or you're hit by a bus, someone else needs access. Document key locations in a sealed legal document with your attorney.

Trade-off: lawyer fees.

Common mistakes & pitfalls

Mistake — Treating 'it's in Dropbox / Google Drive' as backup.

Fix — It's sync, not backup. Deleted there = deleted everywhere.

Mistake — Single-cloud-provider strategy.

Fix — Vendor failure or account lock = total data loss.

Mistake — Never testing restores.

Fix — Untested backups fail at restore time.

Mistake — NAS reachable from same network with same credentials.

Fix — Ransomware encrypts it too. Use immutable or air-gap.

Mistake — Skipping M365/Google Workspace backup.

Fix — SaaS limited recovery windows mean data is gone after 30-90 days.

Mistake — No documented recovery procedure.

Fix — Three hours of panic during the actual event.

Mistake — Backup runs as admin user reachable from production.

Fix — Service-account compromise = backup compromise.

Pro tips

Pro tip 1. Once a year, do a 'I lost my laptop' exercise from each role.

Pro tip 2. Email yourself the runbook quarterly so a copy lives in your inbox.

Pro tip 3. Use Backblaze B2 with Object Lock — best price/safety ratio for SMB.

Pro tip 4. Encrypt locally before upload. Cloud provider never sees plaintext.

Pro tip 5. Keep the immutable bucket retention longer than your average attacker dwell time — 90 days is a good target.

Frequently asked questions

How much does this cost for a 10-person business?

Hardware: $400-700 one-time. Cloud: ~$10-30/month. Time: ~3 hours setup, ~30 min/quarter ongoing. Cyber insurance discount often pays for it.

Do I need a NAS, or is cloud-only fine?

Local + cloud is far faster for restores. A 500GB file restore from cloud can take 24+ hours; from local NAS, minutes.

What about ransomware that hides for weeks before activating?

That's why retention matters. Keep at least 90 days of versioned backups in immutable storage.

Should I encrypt my backups?

Yes, always. If your cloud provider is breached, encrypted backups are useless to the attacker.

Will my cyber insurance require this?

Most insurers now require: documented backups, tested recovery, MFA, and immutable storage. Aligning to these saves on premiums.

What if I'm a 1-person business?

Same principles, smaller scale: USB external drive (rotated weekly) + Backblaze Personal or B2. ~$10/month.

Can I use my regular file sync (Dropbox/OneDrive) as one of the copies?

Only if you back UP from it to something not connected (NAS, cold cloud with versioning). Sync alone is not backup.

Quick recap — do these in order

DO THIS RIGHT NOW

The 8-step recap.

1. Inventory what needs to be backed up.
2. NAS for fast local restores (Synology, QNAP).
3. Encrypted cloud backup (Backblaze B2, Wasabi).
4. Add an air-gap copy (USB rotated monthly or immutable storage).
5. Cover SaaS data (M365, Google Workspace, QuickBooks).
6. Document a recovery runbook.
7. Test quarterly with real restores.
8. Annual full-restore drill.

Mini glossary

3-2-1: Three copies, two media, one offsite — gold-standard backup rule.

RTO: Recovery Time Objective — how fast you can be back up.

RPO: Recovery Point Objective — how much data loss is acceptable.

Immutable / WORM: Write Once Read Many — data cannot be deleted before retention expires.

Air-gap: A backup not reachable from the production network.

Bare-metal recovery: Restoring a full system to fresh hardware from an image.