CICADA | RESOURCES

DATA | 90 MIN | ESSENTIAL | UPDATED NOVEMBER 2026

Back up like ransomware is coming

Three copies, two media, one offline or immutable. Plus the settings that stop a bad day becoming a closed business.

The short version

- ✓ Cloud sync is not a backup, deletions and ransomware replicate.
- ✓ Keep one copy offline or immutable, with separate credentials.
- ✓ Cover email, finance and customer records, not just documents.
- ✓ An untested backup is a hope, not a plan.

Decide what would hurt

Start with the data you'd need to open tomorrow: customer and client records, quotes and invoices, accounting and payroll, contracts, staff files, website content, and the mailbox. Then add the things people would mourn: photos, design files, years of history.

Write down, for each, how much you can afford to lose (an hour? a day?) and how quickly you'd need it back. That sets the frequency and the budget.

Build the 3-2-1

- **Three copies:** the live system plus two backups.
- **Two media:** for example cloud storage plus a local drive or NAS.
- **One offline or immutable:** disconnected when not in use, or locked so it can't be altered for a retention period.

Versioned cloud storage with object lock, a rotated external drive kept in a different building, or a managed backup service with immutability all work. What

matters is that an attacker with your normal admin account can't delete it.

Close the obvious holes

- Use a **separate account** for backups, with MFA, not the owner's daily login.
- Turn on **version history** and a retention period long enough to notice an intrusion, 30 days minimum, 90 better.
- **Alert** on backup failures and on mass deletion.
- Keep **recovery keys offline**.
- Don't leave the only copy on the same NAS or cloud tenant as the live data.

> COMMON FAILURE
>
> The backup ran every night for two years, into a folder the ransomware could also reach. Offline or immutable is the detail that matters.

Write it down

Record the tool, the schedule, retention, who owns it, where the keys are and the last restore test. Keep a copy with your incident card. If the person who set it up leaves, the plan must still make sense to someone else.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.

Action checklist

- [ ] Critical data and systems listed
- [ ] Automatic backups running
- [ ] One copy offline or immutable
- [ ] Backup account separate and protected with MFA
- [ ] Version history and retention enabled
- [ ] Failures alert to a monitored inbox

0 of 6 done