CICADA | RESOURCES

LESSON 02 OF 04 · 8 MIN · ESSENTIAL

Design a backup that survives ransomware

Start from how much you can lose and how long you can be down, then build backwards.

Two numbers to agree

RPO (recovery point objective): how much data can you afford to lose? An hour? A day? A week? That sets the backup frequency.

RTO (recovery time objective): how long can the business be down? An hour? Two days? That sets the recovery method and how much you rehearse it. Write both down; they focus the budget.

The pattern

Three copies, two media, one offline or immutable. In practice: live data, a local or cloud backup for fast recovery, and an isolated copy for the bad day. Add version history long enough to notice a slow intrusion (30 days minimum, 90 better).

Protect the backup account with MFA and separate credentials. Alert on failures and on mass deletion. Keep recovery keys offline.

What to include

Email, finance, customer records, payroll, contracts, website content and the configuration needed to rebuild. A backup of files without the email and the accounts package is half a recovery.

For cloud-only businesses, check the provider's native retention. It is often shorter than you think, and it is not a substitute for your own copy.

> THE ATTACKER'S ADVANTAGE

> Ransomware looks for connected backups first. If your backup is a mapped drive with the same admin credentials as everything else, assume it will be encrypted too.

Key takeaways

- ✓ Agree RPO and RTO before choosing tools.
- ✓ Keep one copy offline or immutable with separate credentials.
- ✓ Include email, finance and configuration, not just files.
- ✓ Alert on failures and mass deletion.

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