CICADA | RESOURCES

LESSON 01 OF 03 · 7 MIN · WORKING KNOWLEDGE

A plan made of decisions

Good incident plans are short because they answer questions, not because they skip them.

Decisions, not documents

In the first hour, someone has to decide: do we disconnect everything, do we pay, do we tell customers, who talks to the bank? A plan exists to make those decisions faster and with the right people.

Name a lead and a deputy. Give them explicit authority to isolate systems and authorise emergency spend up to a limit. Write it down so nobody has to negotiate hierarchy at 8am.

Five roles, shared if needed

- **Lead**: decides and coordinates.
- **Technical**: IT provider or whoever understands the systems.
- **Finance**: bank, insurer, payments.
- **Communication**: staff, customers, suppliers, media.
- **Scribe**: timeline and decisions.

In a five-person business, one person may hold three roles. What matters is that each role has a name and a backup.

Test with a tabletop

Forty-five minutes, one scenario, the people named. “The bookkeeper's laptop shows a ransomware note and the shared drive won't open.” Walk the page. You'll find wrong numbers, missing roles and assumptions. Fix them while it's cheap.

Repeat annually, and after any major change.

THE PLAN MUST WORK OFFLINE

If email and file storage are unavailable, a plan stored only in SharePoint is not available. Print two copies and keep one away from the office.

Key takeaways

- ✓ Name a lead, a deputy and clear authority.
- ✓ Assign five roles; combine them in a small team.
- ✓ Test with a 45-minute tabletop.
- ✓ Keep printed copies available offline.