LESSON 03 OF 03 · 6 MIN · WORKING KNOWLEDGE

After the incident

Recovery is not the end. The weeks after decide whether you get hit the same way twice.

Recover, then review

Once systems are back, hold a review within a week while memories are fresh. What happened, how did we find out, what worked, what slowed us down, what would we do differently? Keep it blameless, the goal is a better system, not a culprit.

Turn the answers into a short list with owners and dates. A review with no actions is a meeting.

Close the entry point properly

Confirm the initial access route is closed, credentials are rotated, sessions revoked, malware removed and backups clean. Watch for recurrence for a few weeks: unusual sign-ins, new inbox rules, odd outbound traffic.

If personal data was involved, complete any regulatory follow-up and be ready to explain what you've changed.

Communicate honestly

Tell staff what happened at a level they need, and tell customers if their data or money is affected. Avoid speculation and don't minimise. A clear, timely message protects trust more than silence does.

Update the incident card, the contact list and the training. Then test the plan again.

> INSURERS ASK

> Claims often require evidence of what happened and what controls were in place. Your timeline, decision log and restore records make the difference between a smooth claim and a difficult one.

Key takeaways

- ✓ Review within a week, blamelessly.
- ✓ Turn findings into owned actions with dates.
- ✓ Confirm the entry point is closed and monitor for recurrence.
- ✓ Communicate clearly and update the plan.

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