

ILLUSTRATIVE CASE STUDY

From Unclear Roles to Coordinated Incident Readiness

Incident response planning and tabletop exercise for a growing organization

INDUSTRY	ORGANIZATION	WORKING MODEL	ENGAGEMENT
Technology-enabled services	100-250 employees	Hybrid and cloud-first	Incident response readiness

Client Context

A growing technology-enabled services organization depended on cloud applications, remote access and third-party platforms to deliver critical services. Security tools were in place and the IT team could handle routine technical issues, but the organization's ability to coordinate a significant cyber incident had never been tested.

The Challenge

The incident response plan did not clearly define decision authority, executive escalation or coordination with legal, privacy, communications and external providers. Important actions still depended on individual knowledge, while recovery priorities and after-hours contacts had not been validated through a realistic exercise.

Engagement coverage: response governance | activation and escalation | ransomware scenario | evidence preservation | communications | legal and privacy | third parties | recovery

How Amnix Approached the Engagement

STAGE	FOCUS	WHAT AMNIX DID
01	Review readiness	Reviewed the response plan, contact lists, recovery dependencies and existing technical procedures.
02	Design the scenario	Built a realistic ransomware and data-exfiltration scenario around the organization's operating environment.
03	Facilitate the exercise	Guided technical and executive participants through escalating decisions, communications and recovery priorities.
04	Convert lessons into action	Documented gaps, clarified responsibilities and developed a prioritized readiness improvement roadmap.

WHAT THE EXERCISE REVEALED

The key gap was not technical capability alone, but coordinated decision-making under pressure.

Priority Themes

Decision authority. Authority to declare an incident, isolate systems, accept downtime and activate external support was not clearly assigned.

Escalation and communication. Triggers and owners for notifications, executive updates and external communications needed definition.

Technical response and evidence. Containment, logging and evidence preservation needed to operate through a repeatable workflow.

Recovery and third parties. Recovery priorities and coordination with cloud, legal, insurance and response providers needed validation.

From Plan to Tested Readiness

BEFORE THE EXERCISE	AFTER THE EXERCISE
Response depended heavily on individual knowledge, with unclear escalation, untested decision points and inconsistent third-party coordination.	Leadership had defined improvement priorities, clearer response roles and a tested basis for coordinating technical and business decisions.

What Amnix Delivered

- An updated incident response plan with activation criteria, escalation paths and defined responsibilities.
- Executive and technical decision guides for containment, communication, evidence and recovery.
- A tabletop after-action report and prioritized roadmap for continued readiness testing.

Business Impact

Technical and business leaders gained a common response model and clearer decision authority. The organization could reduce avoidable delays and align containment and recovery actions with business priorities.

Would your team know what to do in the first hour?

Amnix Advisory helps organizations develop, test and improve incident response capabilities before a real event puts them under pressure.

[Discuss Incident Response Readiness >](#)