GRAENNLAB Strategic Implementation Lab

CASE STUDY

Crisis Management and Cyber Response Integration

Embedding incident response capability into business continuity, escalation, and recovery operations.

CYBER RESILIENCE	BUSINESS CONTINUITY	INCIDENT RESPONSE

POSITIONING LINE
Graennlab integrated cyber response into the operating model, turning incident response from an external service into a documented, actionable recovery capability.

Work Type	Cybersecurity response integration and business continuity governance
Client Need	Operational integration of third-party incident response into crisis and recovery procedures
Graennlab Role	Framework designer, escalation model owner, runbook and recovery workflow contributor
Core Deliverables	Crisis framework, cyber incident procedures, recovery playbooks, status forms, escalation structures

Client Challenge

Clients often have access to security responders but lack an operational model that defines when and how those responders are engaged during a crisis. The work tied to client centered on making a cybersecurity response partner part of the business continuity, crisis management, and recovery model rather than leaving it as an external, ad hoc escalation resource.

Graennlab Approach

Graennlab connected incident response with crisis management and business recovery. The work defined client's role as an incident response coordinator, embedded the security response function into escalation paths, built procedures for suspected or confirmed cyber events, and created practical templates and recovery

structures that could be used during cyber attacks, IT outages, disaster recovery events, and vendor disruptions.

Work Performed

- Defined crisis-management team structure, roles, responsibilities, and command-center model.
- Integrated client into cyber incident escalation procedures and communication protocols.
- Defined cyber incident procedures covering detection, assessment, activation, containment guidance, and recovery coordination.
- Built recovery playbooks for workplace loss, IT systems loss, cyber attack scenarios, and vendor disruptions.
- Created operational tools including event status meeting agendas, incident status forms, damage assessment checklists, and notification procedures.
- Established contact and escalation structures including external incident response hotline, IT escalation contacts, and vendor coordination points.
- Supported broader security capability implementation context including endpoint security deployment and tuning support.

Outcome

The client received an integrated response model connecting cybersecurity incident response, crisis management, business recovery, escalation, and operational communications. Client's role was no longer simply vendor availability. It became an embedded part of the client's continuity and recovery governance model.

WHY IT MATTERS
This engagement demonstrates Graennlab's ability to move beyond advice and provide embedded execution, governance, and operational momentum inside client environments.