gruve

SOLUTION BRIEF

Executive readiness tabletop

Prepare the C-suite and board for cyber decisions that cannot wait

01

Business problem

The hardest decisions in a cyber incident don't sit in the SOC—they sit with leadership. Materiality. Disclosure timing. Board escalation. Customer communications. These are executive decisions, and most executive teams have never practiced them together.

When a significant cyber event unfolds, executives may need to determine whether the event is material, when to involve the board, how to balance legal advice with communications timing, and how to protect business continuity while facts are still developing. Yet in many organizations, the technical team has rehearsed more than the leadership team—leaving the highest-consequence decisions to people who have never coordinated them under pressure.

That creates a governance gap as much as a security gap. SEC rules require public companies to disclose a material cybersecurity incident on Form 8-K generally within four business days after determining materiality. NCUA guidance recommends regular tabletop exercises so board and management teams can practice response plans and understand their roles during an incident. Leadership readiness is now part of cyber readiness.

The challenge is intensifying. Ransomware with exfiltration, third-party compromise, identity-centric incidents, AI-enabled social engineering, and unsafe AI behavior can all force business, disclosure, and reputational decisions before the technical facts are settled. Without rehearsal, organizations risk overreacting, underreacting, or losing time while the people who own the hardest decisions work out responsibilities on the fly.

02

Why now

Executive cyber accountability has become more concrete. Public-company leadership teams operate under compressed disclosure timelines, while sector-specific regulators and governance bodies increasingly expect evidence that leadership understands its role in a serious cyber event. Board oversight expectations are expanding as cyber resilience, AI governance, and operational continuity converge into one executive agenda.

The decision environment is getting harder, not easier. IBM's 2026 X-Force reporting and Google's 2026 threat forecasts point to attackers using AI to accelerate reconnaissance, exploitation, and social engineering—compressing the time between initial activity and high-stakes business consequences. Executive teams need to rehearse scenarios where attacker speed, ambiguous evidence, and external scrutiny combine to pressure leadership into fast judgment calls.

AI adds another executive dimension even when it is not the root cause. Boards and C-suites must account for whether internal copilots, prompt workflows, or AI-enabled customer channels affect exposure, communications risk, or governance obligations. OWASP's LLM guidance and NIST's AI risk frameworks reinforce that prompt injection, sensitive information disclosure, and unsafe model behavior create materially different risk questions than traditional security incidents. That makes executive rehearsal more important, not less.

03

Solution overview

Gruve's Executive Readiness Tabletop is built for the leaders who must make business, disclosure, and governance decisions during a cyber event. The engagement simulates a realistic, high-pressure incident and tests how the C-suite, board participants, General Counsel, Communications, and security leadership align on materiality, escalation, public messaging, and continuity decisions when facts are still emerging.

This is not a technical incident-response workshop dressed up for executives. It is an executive decision exercise designed to expose uncertainty around decision authority, escalation cadence, communications sequencing, counsel involvement, and board engagement. Facilitators create conditions in which leaders must practice how they will govern through a serious cyber event—not merely observe how responders might investigate it.

Each inject forces an executive decision—not a discussion or deferral. Decisions must align across legal, communications, and business leadership. Where alignment or clarity is missing, the gap is documented as a finding. This ensures the exercise produces measurable, defensible outputs grounded in observed behavior.

Scenarios are generated through a structured facilitation platform that ensures realism, consistency, and pacing—allowing facilitators to focus on executive decision quality rather than building slides or improvising narratives. AI teammates support inject drafting, event pacing, decision-thread capture, and summary preparation, but the scenario is directed by experienced facilitators and all observations and recommendations remain human-led.

04

How the engagement works

Each engagement follows a repeatable four-phase model designed to produce evidence-backed findings and actionable improvement guidance.

Phase	Activities	Outputs	Who is involved
1. Pre-session intake	Define objectives, threat context, and regulatory drivers. Review current IR and crisis governance plans. Map decision authority: who owns materiality determination, board escalation, legal engagement, and communications sequencing.	Scoping document, decision authority map, scenario parameters	CISO, General Counsel, executive sponsor, engagement lead
2. Scenario configuration	Platform generates scenario using client context, governance structure, and regulatory environment. Injects mapped to specific executive decisions the leadership team must make.	Configured scenario, inject sequence, decision-point map	Engagement lead, facilitator
3. Live session	Facilitator-led, time-compressed executive simulation. Injects delivered in sequence, each requiring a real decision on materiality, disclosure, escalation, or communications. Facilitators observe decision quality, alignment, and gaps in real time.	Decision log, behavioral observations, raw findings	All participating executives and leadership functions
4. Post-session	Executive summary with evidence-based gap analysis. Every finding tied to a specific inject, observed behavior, and decision outcome. Leadership readout with prioritized action plan.	Executive summary, gap analysis, action plan, board-ready readout	Engagement lead, CISO, executive sponsor

05

Solution items

Capability	Description
Executive- and board-centered scenario design	Frames the exercise around the decisions senior leaders actually own: materiality, governance escalation, communications sequencing, and continuity tradeoffs. Scenarios generated through a structured platform for consistency and realism.
Decision-forcing crisis injects	Uses realistic incident evolution to require leaders to act under uncertainty. Each inject forces a decision with a named owner, defined timeframe, and clear communication path. No decision means a documented finding.
Disclosure and communications workflow validation	Tests how Legal, Communications, Finance, Security, and the C-suite align on disclosure timing, messaging, spokesperson authority, and stakeholder sequencing.
AI-assisted exercise support	AI teammates accelerate inject drafting, decision-thread capture, and debrief preparation. Facilitators retain control over interpretation, conclusions, and all recommendations.
Executive debrief and action plan	Board- and leadership-ready summary of observations, decision gaps, and improvement actions. Findings tied to specific injects and observed behavior—suitable for governance, audit, and insurance discussions.

06

Benefits

Benefit	Description
Improved decision speed under pressure	Rehearses the moments where leadership judgment matters most so the team does not lose time to avoidable uncertainty during a live event.
Clear ownership of materiality and disclosure decisions	Named owners for materiality determination, board escalation, external counsel engagement, and communications sequencing—defined before an incident forces them.
Alignment between legal, communications, and executive leadership	Brings Security, Legal, Communications, and the C-suite into one coordinated decision model instead of leaving each function to imagine the response independently.
Defined escalation to board and stakeholders	Clarifies when and how the board is engaged, how external stakeholders are sequenced, and what information leadership needs to support governance decisions.
Governance-ready outputs	Documented record of leadership rehearsal, decision gaps, and improvement actions—structured to strengthen governance, insurance, and oversight conversations with evidence-based findings.

07

Service tiers

Tier	Focus / scope	Key deliverables	Target audience
C-suite readiness tabletop	Executive simulation focused on leadership decisions during a disruptive cyber incident.	Leadership findings summary, decision-gap analysis, next-step actions	CEO staff, CISO, General Counsel, Communications
Board / risk committee readiness tabletop	Cyber-governance simulation for directors or risk-committee members overseeing a high-consequence incident.	Board-ready summary, oversight observations, governance recommendations	Boards, risk committees, senior executives
Disclosure and communications readiness tabletop	Focused exercise for materiality, public communications, customer messaging, and regulator-facing decision paths.	Disclosure-readiness observations, communications improvement plan, executive summary	General Counsel, IR leadership, Communications, Finance

08

Competitive landscape

Competitor	Strengths	Gruve differentiation
Mandiant / Google Cloud	Strong executive and technical tabletop credibility with frontline incident-response experience.	Often oriented toward premium consulting programs. Gruve provides a more focused executive-readiness model with sharper linkage to disclosure, communications, and governance decision-making.
Kroll	Strong legal and crisis-management reputation with broad executive tabletop experience.	Often heavier in process and packaging. Gruve emphasizes concise executive outputs, DFIR-informed realism, and rapid follow-through.
Unit 42 / Palo Alto Networks	Well-known brand for executive, operational, and technical cyber advisory services.	Best suited to broad enterprise advisory relationships. Gruve differentiates through right-sized execution, legal/communications integration, and practical leadership decision rehearsal.
CrowdStrike Services	Strong responder mindset and tailored tabletop delivery.	Often seen through a technical-response lens. Gruve extends into board dynamics, materiality decisions, and communications workflow validation for executive stakeholders.
Immersive Labs / digital crisis-simulation platforms	Effective at recurring digital simulations and scalable decision-practice formats.	Platform-led programs do not replace live facilitator coaching, legal/communications nuance, or board-ready narrative reporting. Gruve delivers facilitator-led executive realism with governance-grade documentation.

09

Gruve differentiators

Built for executive decision-making, not technical response. Designed for leaders who own governance, disclosure, communications, and continuity decisions—not responder teams.

Decision-driven, not discussion-based. Every inject forces a real decision with a named owner, timeframe, and communication path. No decision means a documented finding.

Evidence-based findings. Every observation tied to a specific inject, an observed behavior, and a logged decision—defensible for audit, insurance, and board conversations.

Platform-powered consistency. Scenarios generated through a structured platform ensuring realism, repeatability, and facilitator focus on decision quality.

AI-augmented, human-led. AI improves exercise pacing, reporting speed, and inject realism. All readiness judgments and recommendations remain human-led.

Governance-ready output. Concise, board-ready documentation reflecting observed decisions and alignment gaps—structured for governance, audit, and insurance discussions.

Modern scenario coverage. Handles ransomware, third-party incidents, AI-related exposure, disclosure pressure, and reputational risk in one executive conversation.

10

Case study

A public technology company needed to prepare its executive team and board risk committee for a cyber event that could force rapid decisions on disclosure, customer communications, and continuity. The technical response process was relatively mature, but the senior leadership team had not rehearsed how they would manage a fast-moving incident raising disclosure, communications, and continuity questions simultaneously. The board and executives were also navigating new risk introduced by AI-enabled business processes and a changing communications environment.

What Gruve delivered

Gruve designed and facilitated an executive-focused tabletop built around a ransomware-and-data-theft scenario with third-party complications, involving the CISO, General Counsel, investor-relations and communications leaders, operations leadership, and selected directors.

- Executive-focused scenario design forcing choices about governance escalation, disclosure timing, operational continuity, customer messaging, and third-party dependency management.
- Facilitator-led decision rehearsal using time-compressed injects and evolving facts to surface leadership behavior under uncertainty—not test memorization.
- AI-assisted exercise support to accelerate capture of decision threads and preparation of debrief materials, with facilitators validating narrative and authoring all recommendations.
- Board-ready reporting summarizing governance gaps, decision dependencies, and improvements to executive briefing materials.

Results

- **Clarified timing and ownership** of materiality discussions, board escalation, and external counsel engagement.
- **Identified a gap** between technical update cadence and the information executives needed for communications and governance decisions.
- **Exposed ambiguity** around spokesperson authority and customer-notification sequencing.
- **Produced a concise executive action plan** for refining crisis governance and decision-support materials.
- **Strengthened confidence** that the leadership team could make aligned decisions during a high-scrutiny cyber event.

Prepare your leadership team for the cyber decisions that cannot wait.

See how Gruve's Executive Readiness Tabletop helps the C-suite and board rehearse materiality, communications, and governance decisions before a high-stakes incident forces them.

Website: https://www.gruve.ai/

Email: contact@gruve.ai