gruve

SOLUTION BRIEF

Incident response plan readiness tabletop

Validate roles, escalation, and cross-functional decisions before the real incident

01

Business problem

Incident response plans don't fail because they were never written. They fail at the moment someone must declare an incident, escalate to counsel, notify the insurer, and coordinate communications—simultaneously. The plan exists. The rehearsed ability to execute it under pressure usually does not.

That gap shows up in the connective tissue between functions. Security may know its workflow. Legal may understand its obligations. Communications may have a template. But when those teams need to hand off information, align on timing, and make coordinated decisions in real time, the seams between them are where confusion, delay, and exposure take hold.

IBM's 2025 Cost of a Data Breach research ties lower breach cost directly to faster identification and containment. NIST SP 800-84 describes tabletop exercises as cost-effective tools to validate that plan content is viable and implementable. CISA's tabletop guidance reinforces that even mature teams often find escalation paths, decision thresholds, and communication responsibilities become ambiguous once a scenario starts moving. The problem is rarely the absence of a plan—it is the absence of rehearsed execution across the full group of stakeholders who will need to act.

Underwriters, auditors, and boards have moved past asking whether a plan exists. They want evidence that the people who must execute it have practiced doing so—and that the exercise produced documented findings, not just attendance records.

02

Why now

Readiness expectations have become more explicit and more time-sensitive. NIST SP 800-61 Rev. 3 frames incident response as a broader cyber-risk-management capability that should improve how organizations detect, respond to, and recover from incidents. SEC cyber disclosure rules compress the timeline for public companies to establish facts and align stakeholders—requiring an Item 1.05 Form 8-K generally within four business days after determining materiality.

Regulated and high-consequence sectors face even more direct pressure. NYDFS implementation guidance requires covered entities to train IR staff, test plans with critical personnel, and revise plans as necessary. HHS cybersecurity performance goals call on healthcare organizations to maintain, drill, and update response plans for relevant threat scenarios. The message across frameworks is consistent: preparedness is an operational capability that must be tested and improved, not a static document.

The threat environment reinforces the urgency. Google's 2026 cybersecurity forecast and IBM's 2026 X-Force reporting both point to AI accelerating the speed and scale of attack activity—from reconnaissance through crisis escalation. Ransomware with data exfiltration, identity-centric compromise, third-party supply chain disruption, and AI-influenced incident narratives create multi-front events that overwhelm plans written for simpler, more linear scenarios. A plan that has never been tested against that complexity is a plan that will be tested for the first time during a real incident.

03

Solution overview

Gruve's Incident Response Plan Readiness Tabletop turns a written IR plan into a rehearsed operating capability. The engagement uses a facilitator-led scenario tailored to the client's threat profile, operating model, and regulatory context to test how the organization declares, escalates, coordinates, communicates, and recovers through a realistic cyber event.

The exercise is deliberately cross-functional. Rather than treating the tabletop as a technical walk-through for the SOC, Gruve tests the connective tissue between Security, IT, Legal, HR, Communications, and executive leadership—including severity thresholds, escalation logic, communications timing, counsel engagement, insurer notification, business continuity tradeoffs, and the decision authority model that will govern a serious incident.

Each inject forces a real decision—not a discussion or deferral. Decisions must have a named owner, a defined timeframe, and a clear communication path. Where the team cannot produce a clear decision, the gap is documented as a finding. This ensures the exercise produces measurable, defensible outputs grounded in observed behavior rather than subjective commentary.

Scenarios are generated through a structured facilitation platform that ensures realism, consistency, and pacing—allowing facilitators to focus on decision quality rather than building slides or improvising narratives. AI teammates support scenario branching, inject drafting, note capture, and after-action report preparation, but facilitators and DFIR leaders control the exercise and all observations, findings, and recommendations remain human-authored.

04

How the engagement works

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

Phase	Activities	Outputs	Who is involved
1. Pre-session intake	Define objectives, threat context, and regulatory drivers. Review current IR plan. Map decision authority: who owns incident declaration, escalation, legal engagement, insurer notification, and communications.	Scoping document, decision authority map, scenario parameters	CISO, IR lead, Legal, engagement lead
2. Scenario configuration	Platform generates scenario using client data, IR plan structure, and scenario modules. Injects mapped to specific cross-functional decisions the organization must make.	Configured scenario, inject sequence, decision-point map	Engagement lead, facilitator
3. Live session	Facilitator-led, time-compressed exercise. Injects delivered in sequence, each requiring a real decision on escalation, coordination, or communication. Facilitators observe and log behavior, decisions, and gaps in real time.	Decision log, behavioral observations, raw findings	All participating functions
4. Post-session	Structured After Action Report (AAR) with evidence-based gap analysis. Every finding tied to a specific inject, observed behavior, and decision outcome. Leadership readout with prioritized remediation roadmap.	AAR, gap analysis, remediation roadmap, executive readout	Engagement lead, CISO, executive sponsor

Every inject forces a real decision—not a discussion or deferral. Decisions must have a named owner, a defined timeframe, and a clear communication path. Where the team cannot meet that standard, the gap is documented as a finding. This ensures the exercise produces measurable, defensible outputs grounded in observed behavior.

05

Solution items

Capability	Description
Scenario design aligned to your IR plan	Builds the exercise around the client's current incident response plan, operating environment, regulatory pressures, and likely threat scenarios—ensuring the session tests actual readiness, not generic theory. Scenarios generated through a structured platform for consistency and repeatability.
Cross-functional decision validation	Tests how Security, IT, Legal, HR, Communications, and leadership hand off information, make decisions, and escalate under pressure. Validates the connective tissue between functions, not just individual team performance.
Decision-forcing facilitator injects	Uses realistic event progression and adaptive injects to force real decisions at each stage. Each inject requires a named owner, a defined timeframe, and a communication path. Where no clear decision emerges, the gap is documented as a finding.
AI-assisted exercise support	AI teammates accelerate scenario branching, inject drafting, decision capture, and reporting preparation. Facilitators and DFIR leaders retain control over interpretation, conclusions, and all recommendations.
After-action reporting and remediation roadmap	Delivers a structured findings package with evidence-based gap analysis, prioritized readiness gaps, and plan-improvement guidance. Every finding tied to a specific inject and observed behavior—suitable for governance, audit, and insurance discussions.

06

Benefits

Benefit	Description
Clear ownership of declaration and escalation	Named owners for incident declaration, escalation, and notification. Defined thresholds for engaging legal counsel, insurers, communications, and executive leadership—documented before a live incident forces them.
Validated cross-functional coordination	Identifies breakdowns in the handoffs, timing, and decision dependencies between Security, IT, Legal, HR, Communications, and leadership—the gaps that create delay in a real event.
Evidence-backed gap identification	Every finding tied to a specific inject and observed behavior—not subjective commentary. Outputs are defensible for audit, insurance, and governance conversations.
Faster time to coordinated action	Shortens the time teams need to organize, escalate, and coordinate because critical decision paths have already been practiced under realistic conditions.
Actionable remediation roadmap	Converts exercise findings into prioritized improvement actions tied to named owners, defined timeframes, and plan revisions—replacing static observation lists with operational follow-through.
Audit- and insurer-ready documentation	Produces documented evidence of testing and improvement that strengthens governance, insurance, and regulatory conversations with evidence-based findings.

07

Service tiers

Tier	Focus / scope	Key deliverables	Target audience
Core IR plan readiness tabletop	Single-scenario validation of the current incident response plan and escalation model.	After-action summary, readiness gaps, prioritized improvement actions	CISOs, IR leads, IT and Legal stakeholders
Expanded cross-functional readiness tabletop	Broader exercise including Security, Legal, HR, Communications, and business continuity dependencies.	Detailed findings report, role clarification matrix, remediation roadmap	Security leadership, HR, Communications, risk teams
Sector / regulatory readiness tabletop	Plan validation tuned to industry-specific decision pressures such as disclosure, patient safety, or regulated data handling.	Sector-specific observations, disclosure/escalation findings, executive summary	Regulated industries, General Counsel, compliance leadership

08

Competitive landscape

Competitor	Strengths	Gruve differentiation
Mandiant / Google Cloud	Enterprise consulting bench, frontline threat intelligence, realistic tabletop experience.	Often packaged as broader premium consulting. Gruve offers a more agile, right-sized readiness model with cross-functional facilitation, evidence-based scoring, and concise remediation outputs.
CrowdStrike Services	Strong responder mindset and brand familiarity for incident response.	Gruve tests decision quality across Legal, HR, Communications, and governance—not primarily the responder team. Better suited for cross-functional plan validation rather than a primarily responder-centric exercise.
Kroll	Deep cyber and legal credibility, broad tabletop experience.	Often heavier in delivery model and documentation. Gruve combines legal and crisis alignment with a repeatable platform, structured scoring, and faster delivery without losing defensibility.
Unit 42 / Palo Alto Networks	Well-known brand for executive and operational cyber advisory services.	Often optimized for broad enterprise relationships. Gruve offers more focused readiness validation with a tighter bridge from exercise output to plan revision and operational follow-through.
Immersive Labs / simulation platforms	Scalable crisis simulations, dynamic scenarios, and repeatable digital delivery.	Platform-led programs do not replace facilitator-led plan surgery, stakeholder coaching, and counsel-ready narrative reporting. Gruve delivers expert facilitation plus actionable governance outputs.

09

Gruve differentiators

Operational proving ground. Tests the full cross-functional response process—from incident declaration through escalation, coordination, and recovery—not just the technical workflow or executive decision layer alone.

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.

Cross-functional by design. Tests Legal, HR, Communications, and executive leadership alongside Security and IT—because real incidents require all of them to coordinate, not operate in parallel.

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

Platform-powered repeatability. Scenarios generated through a structured platform ensuring consistency, speed, and facilitator focus on decision quality rather than slide building.

AI-augmented, human-led. AI improves scenario variation, reporting speed, and note consolidation. All readiness judgments and recommendations remain human-authored.

Connects directly to plan improvement. Exercise observations link to specific plan revisions, stakeholder responsibilities, and operational follow-through—so the exercise produces durable readiness improvement, not just observations.

Built by DFIR practitioners. Designed by professionals who understand how real incidents unfold, not by generic workshop facilitators.

10

Case study

A regional healthcare provider needed documented evidence that its incident response plan was ready for both cyber-insurance renewal and leadership oversight. The organization had a written plan, but it had not been exercised end to end with the full group of stakeholders who would need to act during a real cyber event. Security understood the technical workflow, but Legal, Communications, operational leadership, and compliance oversight had not tested how a disruptive incident would move across their functions. Patient operations and third-party dependencies raised the stakes for decision timing.

What Gruve delivered

Gruve facilitated a ransomware-and-third-party-disruption tabletop involving Security, IT, Legal, Compliance, Communications, and operations leadership to validate how the organization would declare an incident, escalate decisions, and manage stakeholder communications under pressure.

- Reviewed the client's existing IR plan, escalation paths, and stakeholder roles, then built a scenario reflecting the client's actual operating risk.
- Moderated the exercise to force timing-sensitive decisions about incident declaration, counsel engagement, internal communications, and leadership escalation—rather than discussing those issues in the abstract.
- Used AI teammates to accelerate note consolidation and reporting preparation, with facilitators and DFIR leaders validating all observations and authoring the final conclusions.
- Delivered a prioritized remediation roadmap covering the contact tree, escalation model, and communications path so the exercise translated into durable improvement.

Results

- **Identified two escalation-path gaps** and one incident-declaration threshold that would have delayed executive involvement during a live event.
- **Clarified engagement timing** for outside counsel, the insurer, and communications leadership relative to technical containment activity.
- **Produced a documented after-action report** that leadership could use for insurance and governance conversations with evidence-based findings.
- **Created a prioritized update plan** for the IR playbook, contact tree, and role assignments—converting a static plan into a more rehearsed and workable operating process.

Turn your incident response plan into a practiced response capability.

See how Gruve's Incident Response Plan Readiness Tabletop helps your teams validate escalation, coordination, and decision-making—and create defensible evidence of readiness before the real incident arrives.

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

Email: contact@gruve.ai