CyberResponse: The First 72 Hours

A Cyber Incident Leadership Response Simulation

The Brief

A mid-sized financial services firm faced a growing board-level concern: if a major cyber incident struck, would the senior leadership team know how to coordinate an effective cross-functional response? Technical teams had playbooks, but executives lacked practical experience of the real-time trade-offs between containment, regulatory compliance, stakeholder management, and business continuity.

The Goal: The simulation had to force senior leaders to experience the collision of competing priorities during a ransomware crisis — making visible the consequences of delayed communication, regulatory non-compliance, and single-track technical thinking — all within a realistic 72-hour compressed timeline.

Key Objectives: Cross-Functional Coordination, Regulatory Awareness, Stakeholder Management, Resource Prioritisation under Pressure, and the Ransom Dilemma.

The brief specified a 3-hour format for 8-20 participants organised as 2-4 teams of 4-5, with cross-functional roles driving natural tension between IT, Legal, Communications, and Operations.

The Solution

Teams assume the role of a financial services executive crisis team responding to a ransomware attack over six rounds, each representing 12 hours. They manage nine interconnected board metrics — system integrity, data exposure, operational continuity, four stakeholder groups, containment progress, and regulatory compliance — while allocating scarce Action Points and a finite budget across four competing response categories.

Core Mechanic: The Degradation Clock

Until the team achieves containment, every round automatically degrades system integrity, increases data exposure, and erodes stakeholder confidence. The longer containment takes, the worse the compounding damage — making every delayed decision visibly costly on the board.

Key Feature: The Regulatory Clock

ICO and FCA notification deadlines run in parallel with the technical crisis. Filing early earns maximum compliance points; filing late incurs fines. Teams must decide whether to divert leadership attention from containment to compliance — exactly the tension real incident response teams face.

The Ransom Dilemma

A mid-game event forces the team to confront a direct ransom demand with four mechanically distinct options — negotiate, refuse, report to law enforcement, or stall. No option dominates; each creates different downstream consequences across stakeholder confidence, regulatory standing, and containment progress.

Assessment

Independent AI Assessment Score: 92/100

Dimension	Score
Mechanical Quality	23/25
Strategic Depth	23/25
Educational Value	24/25
Playability	22/25

Scored by Claude (Anthropic) using a structured playtest methodology: the AI independently played the full simulation, calculated scores using the documented rules, and evaluated across four standardised dimensions.

Alignment with Learning Objectives

The simulation directly operationalises the cross-functional coordination challenge identified in the brief. Because each action consumes limited Action Points, teams quickly discover that no single department can dominate the response — effective crisis management requires simultaneous attention to technical containment, legal obligations, stakeholder communication, and business continuity. The regulatory clock creates genuine urgency around ICO and FCA notification timing, while the stakeholder confidence system forces teams to actively manage reputation alongside the technical response.

Facilitation Design

The facilitator documentation provides clear guidance on setup, round sequencing, scoring, and debrief discussions. The simulation is designed for a single facilitator but runs more smoothly with two sharing operational responsibilities. Participant materials are

sufficiently clear to support decision-making during play, with role briefing cards ensuring each team member brings a distinct functional perspective to the table.

Mechanical Rigour

The simulation was independently playtested by AI across multiple strategic profiles, confirming that every decision card and event response produces quantified, unambiguous outcomes. The scoring formula's weighted balance across six dimensions (containment speed, regulatory compliance, stakeholder confidence, operational continuity, financial impact, and recovery time) prevents any single-function strategy from dominating. Technical-only approaches cap around 55 points; balanced strategies with early regulatory focus can reach 70+.

Structural Excellence

The six-round structure maps precisely to the 72-hour GDPR notification window, creating a natural narrative arc from initial detection through escalation to resolution. The degradation clock — where uncontained attacks automatically worsen each round — makes the cost of delayed action physically visible on the board. The event sequence escalates authentically: media enquiries, threat actor contact, employee data breaches, board demands, and insurance documentation requirements arrive in a credible order that mirrors real incident timelines.

Summary Specifications

Attribute	Detail
Duration	3 hours (half-day format)
Participants	8-20 (2-4 teams of 4-5)
Domain	Cyber Security Incident Management
Complexity	Intermediate-Advanced (Executive level)
Core Mechanics	Action point scarcity, degradation clock, regulatory timing bonuses, stakeholder erosion, cross-functional decision cards
Physical Components	Crisis dashboards, event cards, decision cards, reference cards, role briefing cards, tokens, cubes, pawns
Facilitator Requirement	L&D professional (no cyber security expertise required)

CyberResponse: The First 72 Hours was developed as a demonstration simulation to showcase The Sim Smithy's capability for translating complex crisis management scenarios into engaging, decision-driven learning experiences.