Facilitating Cyber Crisis Tabletop Exercises: Insights from the Front Line of Simulation Leadership

by Simon Hodgkinson, Presented by Semperis

Across private industry and the public sector, organisations are confronting an unprecedented level of operational risk originating from sources outside their control.

In the cyber space, threats rapidly evolve in scale, sophistication, and impact. Advanced by AI-powered tools and increasingly aggressive criminal groups (e.g., ShinyHunters, Scattered Spider), ransomware, supply chain compromise, identity-based attacks, and data breaches now routinely disrupt operations, reputations, and regulatory standing.

Simultaneously, organisations face increasingly complex and unpredictable threats from geopolitical instability, economic fragmentation, and environmental disasters caused by climate change.

The convergence of these forces has elevated cyber risk to a board-level concern. Organisations are keenly aware that their responsibility is not just to defend against these threats, but to ensure that when a cyber crisis occurs, they are prepared to respond, recover, and resume business operations as quickly as possible.

Decisions made in the first hours of a crisis can shape shareholder confidence, customer trust, brand reputation, and long-term resilience. Even more important are decisions made before a crisis. Planning and preparation are essential for a swift response and speedy recovery.

However, without regular practice, even the best-prepared teams can falter under the pressure of a real-world cyber

incident. A 2025 Semperis study, *The State of Enterprise Cyber Crisis Readiness*, revealed that although 96% of global organizations say they have a cyber response plan, 71% still experienced at least one incident that stopped critical business functions.

96%

of global organizations say they have a cyber response plan,

71%

still experienced at least one incident that stopped critical business functions.

As a facilitator of cyber crisis tabletop exercises, I've stood at the intersection of strategy, psychology, and operational readiness. These simulations are more than technical rehearsals. They are designed to challenge leadership thinking and bridge the gap between the cyber security team, operational leaders, and stakeholders.

This brief provides a firsthand perspective on facilitating tabletop exercises, drawing on real-world experience across sectors. It outlines strategic outcomes, facilitation techniques, and common challenges with the aim of helping executive teams understand the value of simulation-based preparedness and the role of the facilitator in driving meaningful impact.

Although the focus here is on cyber incident response, the insights and learnings are applicable across any crisis. After all, a cyber crisis is just a trigger for a bigger business crisis.

The Facilitator's Perspective

The role of a cyber tabletop facilitator is to guide diverse stakeholders through complex, high-stakes scenarios that test not just systems, but culture, communication, process, and decision making under pressure.

Over the years, I've facilitated exercises across sectors. Each session brings its own dynamics, but the core objectives remain consistent:

- Aligning cross-functional teams
- Maintaining realism
- Ensuring restoration of minimum viable business operations—as soon as possible

To drive these and other meaningful outcomes, the facilitator must ensure all stakeholders, responders, and involved participants emerge from the exercise with:

- A clear understanding of gaps in the response plan
- Steps for continuing to enhance their response processes
- Goals for educating their people
- Trust in their technology decisions

Facilitator Techniques: Setup and Common Challenges

My primary focus during the tabletop exercise is business resilience—not technology.

Businesses constantly change, and the technology platforms, applications, and systems that are in place during this quarter's tabletop or simulation will also change, evolve, or be removed by next quarter. Whether I'm running the simulation for executive or technology teams, I always challenge them to focus on the business outcome: How will we continue to operate during and after this crisis? How will we continue to sell groceries, deliver patient care, drill, or fly planes?

During the exercise, I continually observe, then inject questions to prompt discussion about how actions taken during a crisis will affect the outcome. For instance, how will a particular decision impact our revenue, employees, or brand?

While I go into the exercise with a clear agenda on inject pacing, I also allow flexibility for productive conversation to close "rabbit holes." In those conversations, participants discover critical details and gaps that they aren't aware of,

and working through the questions can clarify the impact of decisions.

The most important piece of advice I would offer is to consider diverse perspectives. I try to draw in the opinions of everyone in the crisis team. Teams must operate in command and control; however, that does not preclude listening to the "quietest voice in the room."

With the objective of business resilience firmly in mind, I move on with the crisis tabletop exercise. Here are four critical challenges that teams typically encounter.

1. VARYING LEVELS OF PREPAREDNESS

I typically start the tabletop with the executive team—and deliberately do not invite technical teams initially.

Executives often arrive with differing assumptions about their role in a cyber crisis. Some expect to delegate; others overstep. This misalignment can stall decision making. During a crisis simulation, a technical team representative provides situation reports and asks for prioritisation while the executive manages the business impact.

In a real crisis, it becomes clear why the separation of the executive team (who are managing the business) and the technical team (who are managing incident response) is critical. It's essential to allow space for the technical team to focus on containment and recovery. Communication and collaboration at the *right time* in the *right context* is key to success.

In a recent tabletop exercise with a multi-billion-dollar company, we spent significant time at the outset outlining roles, expectations, and escalation paths. While this could have been achieved through a pre-brief, walking through the process helped everyone understand why it's important to establish clear roles, responsibilities, and delegation *before* a crisis happens. In this case, the CEO stepped in and appointed one of the team as Crisis Director; through the exercise we were able to remind the CEO that his input was valuable but that he was not the decision maker.

Throughout the exercise, the injections progressively escalate to provoke robust discussion—and here we see the true depth of preparation to make on-the-spot decisions that directly affect not only the crisis outcome but also business resilience and continuity.

For example, the classic question to inject, from a cyber perspective, is, "Who decides if we pay a ransom, and on what basis do we make that decision?"

In a tabletop exercise, it is easy to take the moral and ethical position that the company will never pay ransom. At this point, I turn up the pressure to challenge that assumed response with real-world examples of companies that have lost their digital platform for weeks. I ask, "Would this business be able to survive?"

The answers are not always clear cut, and the reasoning behind decisions is affected by multiple variables. The 2025 Ransomware Risk Report from Semperis reveals that bad actors are constantly finding new ways to force ransom payments.

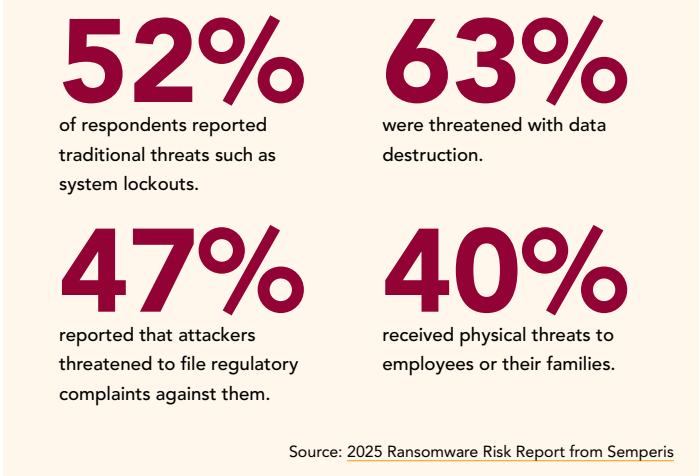
- 52% of respondents reported traditional threats such as system lockouts.
- 63% were threatened with data destruction.
- 47% reported that attackers threatened to file regulatory complaints against them.
- 40% received physical threats to employees or their families.

Cyber crisis preparation must include understanding of both the business impact and the human impact. That leads us to the second common challenge.

2. OVEREMPHASIS ON TECHNOLOGY

In both executive and technical cyber crisis tabletop exercises, there's a tendency to default to discussing technology while neglecting reputational, legal, and human dimensions. The technology is only as good as the process and the people managing and using it.

Methods of Bad Actors in Finding Ways to Force Ransom Payments



Source: 2025 Ransomware Risk Report from Semperis

The best tabletop scenarios focus on non-technical stresses on decision making, such as:

- Media leaks
- Shareholder pressure
- Environmental disasters
- Safety

I ensure legal, communications, HR, and business leaders are active participants, not observers. We must remember the cybersecurity team is generally doing incident response on a daily, weekly, and monthly basis. They know what to do. Where they need the most help is in focusing on operational priorities—and ensuring they have the support of the leadership team and stakeholders.

For example, in a tabletop exercise I conducted for a major UK firm, a simulated ransomware attack prompted heated debate—not about recovery, but about whether to inform the regulator and suppliers. The participants critically ignored the employees despite the HR Director's protestations. The takeaway for them was that it is critical for the incident commander to make sure all voices are heard.

It is also critical to make sure all voices know their roles before, during, and after a cyber incident. Lessons learned come from all participants, not just the cybersecurity team. Keep in mind, while cyber teams are responding and managing the technical aspect of the incident, forensics, logging, and so on, business stakeholders are focusing on trying to keep the business running as technology is restored.

3. DECISION PARALYSIS UNDER PRESSURE

As the tabletop exercise progresses and the injections escalate, the time window reduces, increasing the pressure on decision makers. This can lead to paralysis.

For example, a bad actor may escalate pressure by increasing the ransom demand, informing the regulator, informing your clients, or shortening the deadline for detonation of the malicious payload.

In a simulation, this drives deeper thinking across non-technical teams.

- Communications teams must prepare external and internal communication.
- Legal teams must ensure the right people have been informed in appropriate jurisdictions.
- Business leaders must know how to sustain business operations.

Each response team needs to listen and understand the perspective of the others. How does one reaction or decision impact other teams, services, business lines, and participants?

Often the immediate reaction on the technical side is to shut down external access to the digital ecosystem. However, in today' s world that means the business stops operating. Many high-profile, non-targeted attacks such as NotPetya and WannaCry spread in as little as 20 minutes. The phenomenal pressure that such a timeframe creates makes it clear why designating authority to mitigate cyber risk *in advance* is essential.

For many organisations, that realisation occurs during tabletop scenarios. Empowering the CIO or CISO to respond and contain or mitigate an attack may ultimately save many days—or even weeks—of downtime. However, the reverse should be considered. If they over-respond and impact business operations, it is critical that the reasoning behind the decision is understood so that they are supported and not vilified.

4. ASSUMPTION THAT EXISTING TECHNOLOGY IS AVAILABLE

During most tabletop exercises, the assumption is that standard communication systems will continue to work.

Organisations instinctively reach for familiar tools, only to realise they haven't rehearsed alternatives. Every day, they use email, collaboration apps such as Microsoft Teams, mobile messaging apps, and file sharing platforms such as SharePoint and Dropbox. And they expect those will always be available.

It's likely everyday systems *won't* be available in a crisis. And we must assume that even if these platforms are available, they are compromised—and therefore any communication is freely available to the threat actor.

In a simulation, we quickly establish the need for a totally isolated communications platform. The default tends to be WhatsApp. However, while WhatsApp might serve us well personally, it lacks corporate governance controls, which significantly impacts the forensic investigation and legal discovery process. Likewise, it does not have corporate access and authentication controls, potentially leading to inappropriate access.

Organisations also assume their incident response playbooks will be available; however, they are often on corporate systems that are either shut down or inaccessible when the incident response team isolates the corporate platforms from the internet.

Large, complex organisations also use a variety of tools and systems to communicate with staff and suppliers, and those also may no longer be available—or may create a disjointed response effort.

While none of these system breakdowns would be an issue for a non-cyber crisis, they are a huge issue during a cyber crisis, highlighting the need to prepare a totally isolated crisis management platform. The crisis response platform should be used for cyber and non-cyber incidents so that all teams across the organisation build familiarity.

As a facilitator, my role is to surface these blind spots early, prompting teams to codify contingency channels and ensure that crisis communications can continue even when primary systems are unavailable.

Post-Exercise Debrief

The debrief is a critical part of the tabletop exercise process. I conclude the exercise, take a break for 30 minutes, and ask people to reflect.

While every exercise results in different findings, a few common revelations invariably appear. Organisations discover they must immediately:

- Establish pre-approved communications templates
- Define delegations of authority
- Eliminate over-reliance on individual expertise versus team protocols
- Select and implement an isolated crisis management platform
- Create processes for documenting, logging, and justifying decisions
- Overcome reliance on technology working as it should

Now Is the Time to Transform Crisis Management

A successful cyber crisis tabletop exercise should be challenging and identify gaps in people, processes, and technology. The environment should feel pressurised and uncomfortable for those taking part—because that is the reality of crisis management.

Facilitating cyber tabletop exercises is part art, part architecture. It requires empathy, strategic foresight, and the ability to provoke without destabilising. My goal is always the same: to help leaders rehearse the unthinkable so they can respond with clarity when it counts.

These exercises don't just test systems—they reveal character, culture, and capability. And when done right, *they transform organisations from reactive to resilient*. A reasonable targeted approach is a great starting point. Be focused, be open, and record the critical findings.

Simon Hodgkinson is the former Chief Information Security Officer (CISO) at BP (formerly British Petroleum). He was responsible for cybersecurity including strategy, governance, architecture, education, counter-threat operations, and incident response. Simon currently combines advisory and executive roles for several organisations, including Semperis, Onyxia, Cyera, and ISTARI.

semperis

Run your next tabletop with Ready1

Don't assume your plan will work. Prove it.

- Make **tabletop exercises realistic**—include business leaders.
- Shift focus from more hires to **better coordination**.
- Store and share response plans **in out-of-band systems**.
- **Kill the complexity**: Too many tools = chaos.
- Treat **cyber threats** like any other **enterprise crisis**—because they are.

REQUEST ACCESS TO READY1 TODAY

r1

semperis.com/ready1