WHITE PAPER

REHEARSE TO RECOVER:

Why Confidence Is Not the Same as Readiness

semperis

iSMG

Most organizations believe they are prepared for a crisis.

They have response plans. They have playbooks. They have policies reviewed by legal and approved by leadership. Many have conducted tabletop exercises and audits to satisfy governance expectations or demonstrate due diligence. On paper, they are ready.

And yet, when real crises occur, the outcomes tell a different story.

Business operations stall. Decision-making slows. Roles blur. Communications break down. Executives struggle to translate technical updates into business impact. Teams hesitate not because they lack expertise, but because they have never practiced making consequential decisions together under pressure and with incomplete information.

This gap between confidence and readiness is persistent and structural. Crisis preparedness is often treated as something an organization has, rather than something it must continuously rehearse. Plans exist, but they are rarely tested under realistic conditions. Exercises run, but they are often predictable, narrowly scoped, and limited to the same participants.

Resilience is not a luxury; it's a strategic necessity. But the uncomfortable truth is this: Most organizations do not discover whether they are prepared until the moment they can least afford to find out.

ABOUT THE AUTHOR

Simon Hodgkinson

Semperis Strategic Advisor

Simon Hodgkinson is the former Chief Information Security Officer (CISO) at bp. He was responsible for cybersecurity including strategy, governance, architecture, education, counter threat operations, and incident response. He joined bp in 2002 and has held several senior IT leadership roles. Before becoming CISO, he was the VP for Infrastructure & Integration Services at bp, where he ran Global Infrastructure and Operations across 80 countries, 600 offices, and 75,000 employees. Simon currently combines advisory and executive roles for several organizations, including Semperis, Onyxia, Cyera, and ISTARI.

Decision-Making Is a Crucial Failure Point

When leaders think about crisis response, they often focus on the initial trigger: a cyberattack, a system outage, or a third-party failure.

The assumption is that preparedness depends primarily on detection speed or technical containment. In reality, the most consequential failures occur later.

They occur when executives must decide whether to shut down systems that are still partially functioning. When legal, communications, and operations teams disagree on what can be disclosed, to whom, and when. When uncertainty spreads faster than verified information. When authority is unclear, escalation paths are debated in real time, and every decision carries visible business, regulatory, and reputational consequences.

These moments expose a hard truth. Crisis response is constrained less by technology than by leadership alignment and decision readiness.

Plans rarely fail because they are missing. They fail because they were never tested against the conditions that matter most: time pressure, incomplete information, cross-functional tension, and irreversible trade-offs. This is where many organizations discover that their confidence was misplaced. They had documented procedures, but they had not rehearsed how leaders would decide together when the plan no longer fit the situation unfolding in front of them.

In my experience, this is the point where even well-documented plans begin to break down, not because they are incomplete, but because they have not been tested under the conditions leaders actually face during a crisis.

Real-World Examples

The 2017 NotPetya cyberattack on a major shipping company remains one of the clearest demonstrations of how large organizations lose operational control faster than leadership coordination can keep up.

Within hours, the company's global operations were disrupted across regions and business units, forcing executives to make critical decisions with incomplete information and limited visibility. Coordination across businesses and geographies was crucial in re-establishing minimum viable business processes and providing prioritization to the technical teams who focused on containment and recovery. Ultimately, this incident cost the company hundreds of millions of dollars. The incident established a pattern: When disruption outpaces decision alignment, impact escalates quickly.

And that pattern repeats across industries. In 2024, a major cyber incident triggered widespread disruption across the U.S. healthcare system. The victim was a critical third-party provider that supports claims processing, billing, and pharmacy services for thousands of healthcare organizations. When its systems were taken offline, hospitals, pharmacies, and providers across the country were forced into crisis response simultaneously. Claims processing stalled, prescriptions could not be filled, and revenue cycles were disrupted for weeks. Healthcare leaders were required to make urgent decisions affecting patient care, financial continuity, and regulatory exposure without shared rehearsal for a sector-wide dependency failure. The duration and breadth of the impact underscored how issues with coordination, access, and decision authority can prolong disruption long after an initial incident.

A similar breakdown occurred during a 2022 airline operational crisis. Severe winter weather triggered initial disruptions, but the most significant impact for one airline stemmed from the need to coordinate recovery across its crew scheduling systems and operational teams. Thousands of flights were canceled over several days, stranding passengers and overwhelming customer service channels. Leadership was forced to make high-stakes decisions with limited visibility into crew availability and system constraints. The incident demonstrated how important it is to align logistics, communication, and decision-making under sustained pressure.

The pattern remains consistent. The most damaging consequences are rarely caused by the initial disruption alone. Organizations must ensure that they can make decisions, coordinate disparate teams, and regain access at the moment when they are under the greatest pressure.

Confidence ≠ Readiness

Semperis research highlights a persistent contradiction in how organizations assess their own preparedness.

In Semperis' State of Enterprise Cyber Crisis Readiness report, 96 percent of organizations reported having a cyber crisis response plan. Ninety percent activated those plans in the previous year due to a cyber incident, and most still struggled with serious blockers to effective response. The most significant was limited cross-functional participation in crisis exercises. Fewer than half of organizations regularly conducted tabletops that included all teams involved in a real crisis.

The consequences are sobering. Even with plans in place, 71 percent of organizations experienced at least one cyber incident that disrupted critical business functions in the previous year, and more than one-third suffered multiple damaging incidents. These findings do not suggest that response plans failed to activate, but they do highlight how frequently organizations are required to operate under crisis conditions that test coordination, decision-making, and execution in real time. The question is not whether a major cyber incident will disrupt business functions—it will do—but whether the organization can re-establish critical business functionality quickly and effectively.

Ransomware data reinforces the point. According to the Semperis 2025 Ransomware Risk Report, 78 percent of organizations were targeted by ransomware in the previous 12 months, with nearly three-quarters attacked more than once. Among successful attacks, 69 percent resulted in a ransom payment, often multiple times. These figures reflect the scale and persistence of attacks, as well as the complex decisions organizations must make under pressure when recovery, continuity, and risk converge.

Each of these incidents requires coordinated decisions across security, operations, legal, communications, and executive leadership. The frequency of incidents, combined with the recurring need to make high-stakes decisions under pressure, points to a consistent pattern. Organizations are regularly activating crisis plans, but often under conditions that require teams to adapt, align, and make decisions in ways they have not fully rehearsed.

Confidence is widespread. Readiness is not.

71%

of organizations experienced at least one cyber incident that disrupted critical business functions in the previous year.

Institutionalizing Crisis Readiness

Organizations fail in crises not because they lack plans, but because those plans can't be executed under real conditions.

We've learned that identity compromise is often the tipping point. When access and trust break down, coordination slows, visibility disappears, and leadership decision-making degrades.

Institutionalizing readiness means ensuring rehearsal outcomes do not depend on individual memory or ideal conditions. Plans must be accessible when primary systems are unavailable. Authority and escalation must remain clear even when identity systems are compromised.

This requires preserving institutional knowledge as teams change, testing out-of-band access and communication, and embedding rehearsal into governance rather than treating it as an annual exercise. Organizations that do this build readiness that endures.

Crucial best practices include:

1 Codify Response Under Abnormal Conditions

Crisis response plans are often written with the assumption that systems will be available, credentials will work, and teams will be able to coordinate as usual. Real incidents routinely prove otherwise. When identity systems are compromised, access becomes fragmented. Privileged accounts may be unavailable. Trust relationships may be broken. Responders can be locked out of core systems. Executives lose visibility at the moment they need it most.

This is where many plans collapse.

Institutional readiness requires response plans that are not only documented, but also accessible when primary systems are degraded or untrusted. Roles, escalation paths, and authority must be clearly defined and available even when normal access controls no longer apply. Plans must be current, version-controlled, and aligned with how decisions are actually made during crises, not how they are imagined on paper.

Tabletop exercises should explicitly test these conditions. If leaders and responders can't access plans, contacts, or escalation paths during an exercise, they should assume the same will be true during a real incident.

2 Preserve Institutional Knowledge

Leadership teams change. Responders rotate. Third-party relationships shift. Without a way to preserve institutional knowledge, the lessons surfaced during tabletop exercises are lost, and organizations are forced to relearn the same hard truths during the next crisis.

From a cyber resilience perspective, this is one of the most overlooked risks in crisis preparedness. Readiness is not static. It must survive personnel changes, restructuring, and growth.

Institutionalizing rehearsal means capturing what was learned during exercises and ensuring it informs future decision-making. This includes documenting assumptions that failed, decisions that proved difficult, and dependencies that were previously invisible. Without this, organizations return to confidence without readiness.

3 Establish Out-of-Band Access and Communication

One clear lesson from real incidents is that communication and coordination tools can't be assumed to work during a crisis.

When systems are compromised or intentionally taken offline, leadership teams must still be able to coordinate securely, maintain confidentiality, and sustain command and control. Without out-of-band access and communication, decision-making fragments and response slows.

Effective tabletop exercises must include scenarios in which familiar tools can't be trusted. This forces organizations to confront how they will coordinate when conditions are most constrained.

Semperis sees this failure pattern repeatedly. Organizations that have not rehearsed out-of-band coordination are forced to improvise under pressure, often at significant cost.

4 Support Rehearsal as a Discipline

As organizations mature their crisis preparedness programs, maintaining current plans, enabling secure access, and preserving rehearsal outcomes across teams and regions becomes increasingly difficult to manage manually.

This is where disciplined approaches and supporting capabilities become essential. The objective is not to replace leadership judgment or accountability. Instead, organizations need a way to ensure that crisis plans are available when needed, that identity recovery is addressed explicitly, and that the outcomes of rehearsal inform future response.

Semperis supports this discipline by helping organizations operationalize crisis readiness in environments where identity compromise is assumed, not hypothetical. Drawing on experience from real-world incidents and tabletop exercises, Semperis enables leadership teams to maintain access, coordinate decisions, and sustain response even when identity systems and infrastructure are under attack. The focus on identity recovery and access continuity is what enables rehearsal outcomes to translate into action when conditions are at their worst.

From Insight to Execution

Understanding what to test is necessary, but insufficient. Many organizations run strong exercises, surface gaps, and align on improvements. Then priorities shift, urgency fades, and lessons lose force. Readiness degrades.

Operationalizing crisis readiness requires structures that make rehearsal repeatable and lessons durable, even when identity systems and infrastructure are under attack.

This is where insight becomes execution.

Crisis readiness is proven by how leaders act when assumptions fail, access is constrained, and decisions must be made under pressure. Organizations that rehearse in this way recover faster, decide with greater clarity, and limit long-term damage. Their confidence is grounded in experience, not assumption.

Resilience is not built during a crisis. It is built before one occurs, through disciplined rehearsal that prepares leaders to act when it matters most.

If you've found that your organization's confidence in recovery isn't keeping up with the risks you face today, please reach out to us here, or visit https://www.semperis.com/ready1 to learn more about how we can help you.

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures the integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid identity environments—including Active Directory, Entra ID, and Okta—Semperis' patented technology protects over 100 million identities from cyberattacks, data breaches and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in Hoboken, New Jersey, and operates internationally, with its research and development team distributed throughout the United States, Canada, and Israel.

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

902 Carnegie Center · Princeton, NJ · 08540 · www.ismg.io