The State of Crisis Readiness - How Prepared Is Your Organization in an Era of Continuous Disruption?

Executive Summary - Crisis readiness is no longer a "nice to have"—it is a defining capability of resilient organizations. Yet, despite escalating threats, most corporations remain only partially prepared. Only ~49% of companies have a formal crisis plan. *(Lucey, 2024)* As many as 23% have no crisis plan at all. *(Segal, 2023)* While 75%+ of organizations activated crisis plans in the past year, indicating frequent disruption. *(Rebecca, 2024)* Fewer than 25% regularly test or exercise those plans. *(Lucy, 2024)*

At the same time, the threat landscape is expanding - cyber incidents, supply chain failures, climate events, and reputational risks are converging, often simultaneously.

Key Takeaway: *Most organizations are experiencing crises - but are not fully prepared to respond effectively.*

Crisis Readiness Impacts:

Plan Adoption versus True Preparedness - First, we can draw a distinction between plan adoption and true preparedness. While many organizations report having plans, 61% of businesses globally have a business continuity plan, leaving a large gap in readiness. *(Shulmistra, 2025)* Additionally, 24% of U.S. employees say their company lacks a formal emergency plan. *(Fusion Risk, 2024)* Where plans exist, they are often; outdated, siloed across functions, and not operationalized into workflow.

Reality: Having a plan does not equal being prepared.

Increasing Frequency of Crises - A crisis is no longer episodic - it is continuous. Globally, only about 50% of all organizations have any kind of crisis plan. Of those, 75.1% had to activate it in the past year. *(Rebecca, 2024)* 65% activated emergency communications plans multiple times annually. *(F24, 2024)* Implication for executives: Crisis readiness must be treated as an operational discipline - not a compliance exercise.

The Cost of Poor Preparedness - Today, more than 50% of businesses without effective resilience plans fail after a major disruption. *(Deloitte)* Cyber incidents alone impact approximately 20% of businesses annually. *(Gov.UK, 2025)* Repeated attacks average 30 incidents per year.

Bottom Line: Crisis readiness directly impacts enterprise survival, not just risk posture.

Top 10 Risks Facing Corporations Today

There is an old saying, “trouble comes in threes”. Our reality is that we live in a very interconnect world. A crisis can easily cascade into a “poly-crisis”. Take the blockage of the “Strait of Hormuz” which is impacting 20% of the oil distribution and several other raw resources essential to global supply chains, energy demand, and food supply. One event, many crises.

Survey Says

Any one of these can catapult to a higher risk, but in general and drawing from global risk surveys and crisis activation data, the top enterprise risks for (2025–2026) include:

1. Cyber Incidents
2. Artificial intelligence
3. Supply chain / third-party failure
4. Extreme weather & climate events
5. Regulatory and legal changes
6. Workplace violence & safety incidents
7. Reputational and brand crises
8. Operational / technology outages
9. Geopolitical instability & civil unrest
10. Health crises / workforce disruption

Key Insight: *Most crises are interconnected and cascading, not isolated events.*

The Readiness Gap: Where Organizations Fall Short

Lack of Testing and Training – Less than 25% of organizations actively drill crisis plans. *(Lucy, 2024)* Yet 75% conduct some training annually. *(F24, 2024)* Those that run exercises often do not address specific scenarios or include cross-functional teams. **Gap:** Training exists—but is often not realistic or operational.

Siloed Ownership – Risk management, communications, security, and IT operate independently. There is no common operating picture. Plans are not integrated into a single execution framework.

Limited Executive Engagement - Senior leadership is not consistently involved in exercises and after-action reviews. Only about 46% of organizations conduct formal post-incident reviews *(Rebecca, 2024)*

Failure to Operationalize Plans - Plans often sit in PDFs or static documents. Plans are not role-based, workflow-driven and connected to real-time data.

Best Practices for Crisis-Ready Organizations

Build an Effective Response Framework – Work with a qualified crisis management advisor to do a vulnerability assessment and build a plan that supports a response framework designed for your organization.

Operationalize Plans into Actionable Workflows – Move from static documents to role-based digital playbooks, trigger-based workflows, and pre-approved decision trees.

Integrate Across Functions – Unite key stakeholders representing your response teams (Risk, Security, Communications, Business Continuity, and HR) with shared systems and information to reduce errors and generate a faster, coordinated response.

Build Real-Time Situational Awareness – Automate the collection and routing of incident reports and external threat alerts to response team members. This will enable a faster response.

Prioritize Speed of Decision-Making – Pre-define authorities, escalation thresholds, alert routing, communication templates, and response protocols.

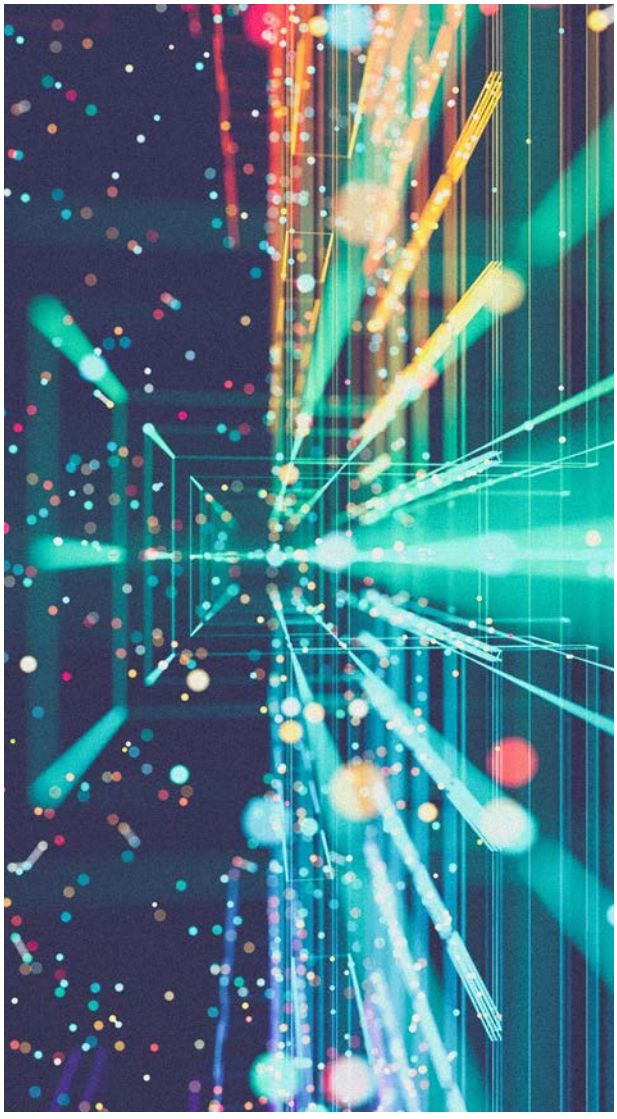
Conduct Scenario-Based Exercises – Move beyond plan training, conduct tabletop exercises that include your cross-functional response teams.

Embed Crisis Readiness into Leadership Culture - Involve executives in simulations, reviews, and strategy. Executive sponsorship and endorsement is critical to a healthy program.

Strengthen Crisis Communications – Build a library of message templates, holding statements, stakeholder maps. This will reduce response times and ensure message consistency.

Implement Continuous Improvement – A healthy program requires timely reviews. This includes after-action reports, plan updates, and incorporation of “lessons learned”.

Leverage Technology Platforms – Avoid the pitfalls of the silo-based, patchwork of tools and invest in a platform that will unify your teams, automate cross-functional workflow, and provide a common operating picture.



The Future of Crisis Readiness

Leading organizations are shifting from:

Traditional Approach

- Static plans
- Siloed teams
- Reactive response
- Periodic testing
- Manual processes

Modern Approach

- Dynamic, digital playbooks
- Cross-functional coordination
- Proactive threat monitoring
- Continuous readiness
- Automated workflows

Conclusion

Crisis readiness is now a core enterprise capability—on par with cybersecurity, financial controls, and compliance.

Despite increased awareness, many organizations remain underprepared. A significant percentage of organizations do not have a crisis plans or operating with incomplete, untested, or siloed one. At the same time, the pace and complexity of crises are accelerating presenting increasing risk.

For operational risk leaders, the mandate is clear:

Move from no plan → to a response framework

Break down silos → enable coordination

Invest in scenario-based exercises → not just training

Organizations that do will not only survive crises—they will emerge stronger, faster, and more trusted.

www.**RockDoveSolutions**.com