semperis

EXECUTIVE SUMMARY

The State of Enterprise Cyber Crisis Readiness

A Global Look at how Organizations Prepare — and Struggle — to Respond to Cyber Threats

Despite widespread claims of cyber preparedness, most organizations aren't battle-ready when it counts. The top blockers? Not staffing shortages. It's **communication breakdowns, plan chaos, and tool overload.**

A global study of 1,000 organizations[1] reveals a disconnect between perceived readiness and actual performance in cyber crisis response.

Practice ≠ Prepared

Plans are being tested — but not holistically. In a real crisis, too many teams operate in silos.

The good news: **96%** have a **cyber crisis response plan**, with most of those fully integrated.

The plan came in handy: **90%** of crisis response teams were activated due to a cyber incident the past year — some more than **25 times.**

Unfortunately, the practice is incomplete: **78%** run **monthly or quarterly tabletops** or audits on their plan, but many **exclude critical teams**:

- × Only **35%** involve legal, finance, or HR
- × Only **37%** include business continuity
- × Only **43%** bring in disaster recovery

When incidents strike, the cracks show. The **study reveals a disconnect** between perceived readiness and real-world performance in cyber crisis response.

Even with practice, **71%** of organizations experienced **at least one high-impact cyber incident** that disrupted critical business functions in the past year; **36%** suffered **multiple major incidents**.

Only 10% **report no serious blockers to effective cyber incident** response. Staffing shortages — surprisingly — came in last among the **top 5 blockers**.

Top 5 Blockers to Effective Cyber Response (Ranked)

1. CROSS-TEAM COMMUNICATION GAPS

2. OUT-OF-DATE RESPONSE PLANS

3. UNCLEAR ROLES AND RESPONSIBILITIES

4. TOO MANY DISPARATE TOOLS

5. STAFFING SHORTAGES

[1] Global study, conducted by Censuswide on behalf of Semperis, of 1,000 organizations in energy, finance, healthcare, IT/telecom, travel/transportation, manufacturing/utilities, education, and government organizations across the US, UK, Australia, New Zealand, Singapore, France, Germany, Spain, and Italy.

What Cyber Leaders Need to Know

Most organizations believe they're ready for a cyber crisis. Repeated business-stopping events say otherwise. Simply hiring more people isn't the answer. To drive resilience, organizations need to fix gaps in cross-team communication and coordination.

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

- Make **tabletop exercises realistic** — and 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 crises** — because they are.

"Some organizations treat breach preparedness as a casual conversation rather than conducting thorough, effective tabletop exercises. A well-intentioned discussion should be used to lay the foundation for meaningful, hands-on exercises that define real readiness."

Jim Bowie
CISO | Tampa General Hospital

"Cyber incidents don't wait for organizations to be ready — they strike when you're least prepared. In a crisis, you don't rise to the occasion. You fall to the level of your preparation."

Marty Momdjian
GM of Ready1 | Semperis

About Ready1

FAIL WITH CONFIDENCE. RUN YOUR NEXT TABLETOP WITH READY1.

Ready1 is an enterprise resilience platform built to empower SOC teams and business stakeholders to measure, manage, and report cyber preparedness, and respond to incidents effectively. Ready1 creates order out of chaos by coordinating and documenting incident response, thus reducing the risk of prolonged downtime, data exposure, financial loss, and regulatory fines.

Learn more at semperis.com/ready1.

Note: Percentages shown reflect global averages. **Read the full report at semperis.com.**