ready1
powered by semperis

The State of Enterprise Cyber Crisis Readiness

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

- Gaps in communication and coordination are blocking effective cyber response — even for organizations that have integrated crisis response plans.
- An overload of disparate out-of-band tools is complicating incident response for many organizations.
- Tabletop exercises often lack input from key cross-team stakeholders and decision makers.

"In today's modern enterprise, operational resilience is the mainstay of effective cyber breach preparedness. It goes beyond just responding to incidents — it's about ensuring the business can keep functioning when systems are under attack or go down entirely."

Jim Bowie
CISO | Tampa General Hospital

Executive Summary

Despite widespread claims of cyber preparedness, pervasive business impacts indicate that most organizations aren't battle-ready when it counts. This global study of 1,000 organizations across the US, UK, Europe, and the Asia-Pacific region reveals a disconnect between perceived readiness and actual performance in cyber crisis response.

Our study reveals that cyber incident response plans are being implemented and regularly tested — but not holistically. In a real-world crisis, too many teams operate in silos.

- **90%** struggle with **serious blockers to effective cyber response.**
- Less than **50%** are **conducting tabletops** that include all the teams commonly involved in an **actual crisis.**
- Even with plans and practice, **71%** still experienced at least one **high-impact cyber incident** that stopped critical business functions in the past year; **36%** suffered **multiple damaging incidents.**

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.

CONTRIBUTING EXPERTS

Chris Inglis
Former US National Cyber Director, Strategic Advisor | Semperis

Jeff Wichman
Director of Incident Response | Semperis

Courtney Guss
Director of Crisis Management | Semperis

Jim Bowie
CISO | Tampa General Hospital

Marty Momdjian
Ready1 GM | Semperis

Table of Contents

Cyber Incident Response in Crisis

The global cost of cybercrime is estimated to reach as much as **$10.5 trillion** in 2025. Clearly, effective cyber incident response must be a key part of proactive crisis management.

To get a pulse on the global state of cyber crisis response, Semperis partnered with research firm Censuswide to conduct a study of 1,000 organizations across the US, UK, Germany, France, Italy, Spain, Australia, New Zealand, and Singapore. We wanted to know:

Is your cyber crisis response plan ready to ensure your business and operational resilience?

When we asked study participants about crucial cyber crisis management steps, their initial responses were encouraging.

96% have a cyber crisis response plan.

83% of those are fully integrated into broader enterprise crisis management planning.

90% of crisis response teams were activated due to a cyber incident in the past year.

But when we asked about the practical details and real-life effects of those organizations' plans, a different — and more chaotic — story emerged.

71% of organizations experienced at least one high-impact cyber incident that stopped critical business functions in the past year.

36% suffered multiple major incidents.

Why aren't companies' cyber response plans driving better business resilience?

"Without ongoing engagement with experienced incident response professionals, teams often build their plans around assumptions rather than real-world threats and trends. That gap becomes painfully obvious during an actual incident."

Jeff Wichman
Director of Incident Response | Semperis

Blockers to Effective Incident Response

Only 10% of study respondents reported no significant blocks to effective cyber response.

Communication gaps led the list of blockers. Without dedicated tools for out-of-band crisis management — considering that a ransomware or other severe attack can disrupt email and messaging systems — teams often struggle to communicate effectively.

Yet only **85%** of organizations said they have such tools, and **21%** didn't use the same tool across all the teams involved in a crisis or were unsure whether they did. (Perhaps not coincidentally, having too many disparate tools was another blocker for many study participants.)

Organizations were also stymied by **outdated response plans.** "Often, companies in crisis find that their playbooks don't reflect the way the business operates," explains Courtney Guss, Semperis Director of Crisis Management.

Jim Bowie, Tampa General Hospital CISO, notes that when plans are outdated or unclear, "the results are almost always chaotic." Unless tailored to the organization's industry and business needs, he warns, plans might focus on compliance — not operational resilience.

To stop breaches from threatening crucial systems and services — and even causing denial of cyber insurance claims — incident response actions must be followed in a specific order by specific people, sometimes including those outside of IT and cybersecurity. But many companies told us they struggle with **unclear roles and responsibilities** during a crisis.

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

"A generic plan might drive people through an unrealistic escalation path that they can't actually implement because it doesn't match their technology, staffing, or budget."

Courtney Guss
Director of Crisis Management | Semperis

When Practice ≠ Prepared

A cyber crisis response plan must be executable at a moment's notice, whatever the threat. That's where practice comes in.

Tabletop exercises should help an organization ensure that its plan will work in practice, not just in theory. Practical application of lessons learned enables the organization to adapt to evolving threats, new technologies, and changing compliance demands.

"Meaningful, hands-on exercises define real readiness," Bowie explains. "Business unit leaders, company executives, and even Board members should be as familiar with their roles and as comfortable executing the plan as the IT and cybersecurity teams are."

To achieve this level of familiarity, cyber response plans need to specify clear, defined roles and responsibilities — not just within the IT and cybersecurity teams, but for crisis decision makers across the enterprise. Tabletop exercises need to put every stakeholder through the paces of practical, realistic cyber crisis scenarios. Yet few organizations are conducting this type of comprehensive exercise.

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

"Do employees across the enterprise know in advance what they can and can't do in the event of a crisis?" asks Marty Momdjian, Semperis Ready1 GM. "That knowledge is key to acting with confidence. Lack of that confidence can cause paralysis — exactly when your business can least afford it."

"In today's cyber threat landscape, the ability to respond swiftly and decisively is just as critical as prevention."

Chris Inglis
Former US National Cyber Director and Strategic Advisor | Semperis

Boost Your Cyber Crisis Response Confidence

"It's important to get a realistic view of your crisis response capabilities so that you can build from there. That requires some honest discussions," says Guss.

Here's how cybersecurity and business leaders can increase confidence in their organization's cyber crisis response plan.

1. **Tailor the plan to serve your organization's needs.** To ensure that your playbooks are tailored to the cyber challenges of your industry and organization, determine the company's risk tolerance, calculate recovery gaps, identify critical assets and Tier 0 resources, and dedicate roles to carry out specific actions in a specific order — not just for IT operations and cybersecurity leadership, but also for your Chief Risk Officer, critical business unit leaders, and even Board stakeholders.
2. **Ensure consistent, secure communications.** To improve cyber crisis response performance, dedicate out-of-band tools for plan storage and crisis communications across the enterprise.
3. **Practice, practice, practice.** Increase your agility by increasing scenario complexity and adding advanced techniques to your tabletop exercises. Adapt playbooks based on the lessons learned. And give plan participants time to adapt to playbook changes.

A robust, integrated, and well-practiced cyber crisis response plan is paramount for cyber and business resilience. "After all," says Momdjian, "the more quickly you can respond and recover, the less severe the financial impact of a cyberattack."

"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
Ready1 GM | Semperis

This global study, conducted by Censuswide on behalf of Semperis, includes responses from **1,000 organizations** across:

- United States
- United Kingdom
- Australia
- Singapore
- New Zealand
- France
- Germany
- Italy
- Spain
- Education
- Energy
- Finance
- Government
- Healthcare
- IT/Telecom
- Manufacturing (MFG)/Utilities
- Travel/Transportation (Transport)

Cyber Crisis Response Plan Implementation + Integration

Do you have a comprehensive cyber crisis response plan?

GLOBAL **96%** Yes

Is your cyber response plan integrated into your enterprise crisis management plan?

GLOBAL **83%** Yes

BY COUNTRY

NEW ZEALAND	98%
SINGAPORE	98%
AUSTRALIA	97%
FRANCE	97%
GERMANY	97%
US	97%
ITALY	95%
UK	93%
SPAIN	91%

BY COUNTRY

US	90%
SINGAPORE	87%
GERMANY	83%
NEW ZEALAND	81%
FRANCE	80%
UK	80%
AUSTRALIA	79%
ITALY	77%
SPAIN	76%

BY INDUSTRY

FINANCE	99%
HEALTHCARE	98%
ENERGY	96%
TELECOM	96%
TRAVEL/TRANSPORT	96%
MFG/UTILITIES	95%
EDUCATION	92%
GOVERNMENT	88%

BY INDUSTRY

IT/TELECOM	87%
ENERGY	86%
FINANCE	83%
TRAVEL/TRANSPORT	80%
EDUCATION	78%
HEALTHCARE	78%
MFG/UTILITIES	77%
GOVERNMENT	52%

What's Preventing Effective Cyber Response?

GLOBAL

1. CROSS-TEAM COMMUNICATION GAPS
2. OUT-OF-DATE RESPONSE PLANS
3. UNCLEAR ROLES AND RESPONSIBILITIES
4. TOO MANY DISPARATE TOOLS
5. STAFFING SHORTAGES

BY COUNTRY		BY INDUSTRY
US, UK, AUSTRALIA, SINGAPORE, SPAIN	CROSS-TEAM COMMUNICATION GAPS	ENERGY, FINANCE, GOVERNMENT, HEALTHCARE, TRAVEL/TRANSPORT, IT/TELECOM, MFG/UTILITIES
US	OUT-OF-DATE RESPONSE PLANS	IT/TELECOM, MFG/UTILITIES
FRANCE, GERMANY	TOO MANY DISPARATE TOOLS	GOVERNMENT
NEW ZEALAND, ITALY	STAFFING SHORTAGES	EDUCATION

Out-of-Band Crisis Management Tools

Do you have dedicated out-of-band tools?

85% Yes

Do incident response, operations, and crisis management use the same tools?

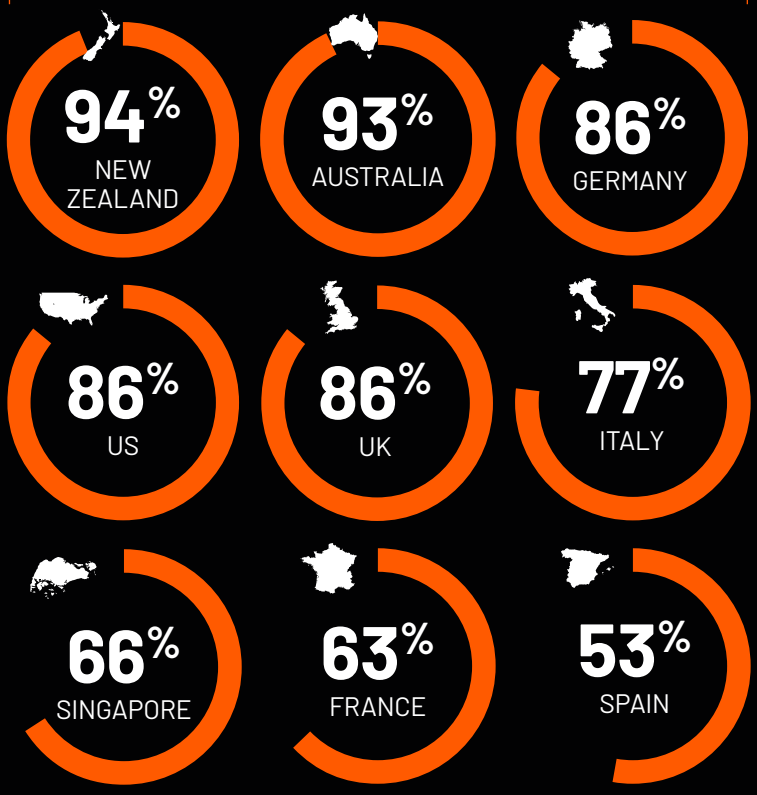
21% No/Unsure

On average, enterprises use 20+ disparate tools for cyber crisis response.

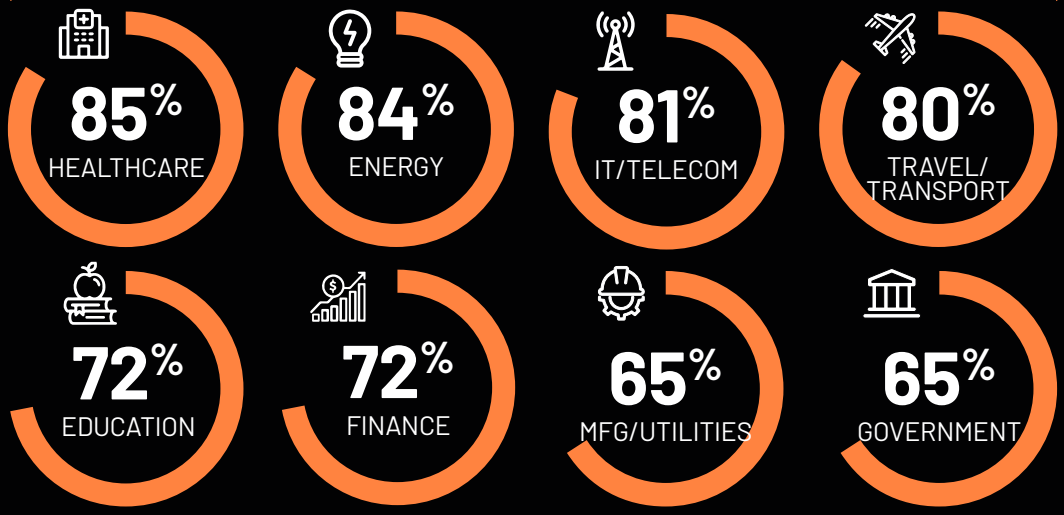
Putting Cyber Response into Practice

How often do you conduct tabletop exercises or response plan audits?

MONTHLY/QUARTERLY TABLETOPS CONDUCTED

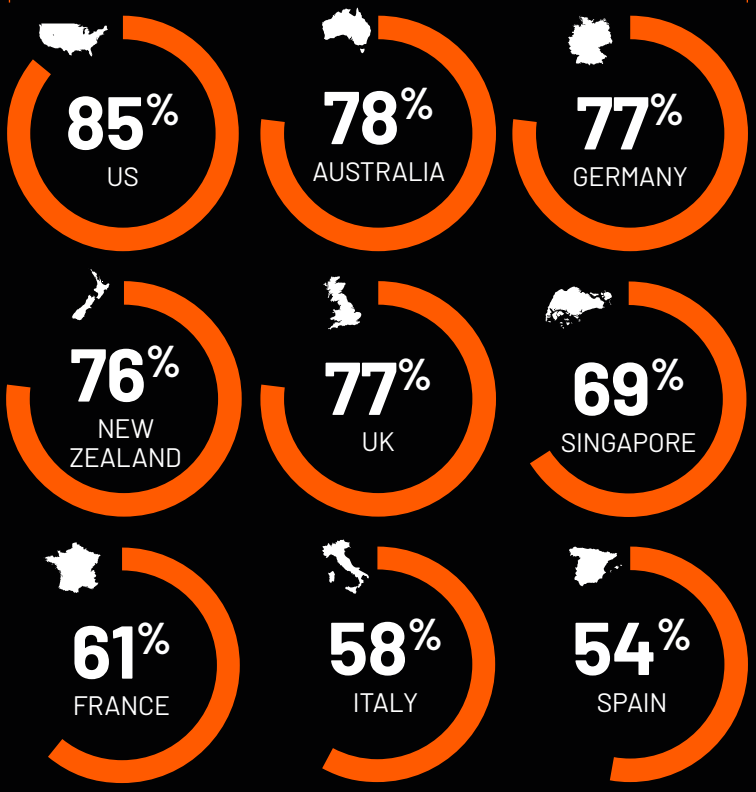


MONTHLY/QUARTERLY TABLETOPS CONDUCTED

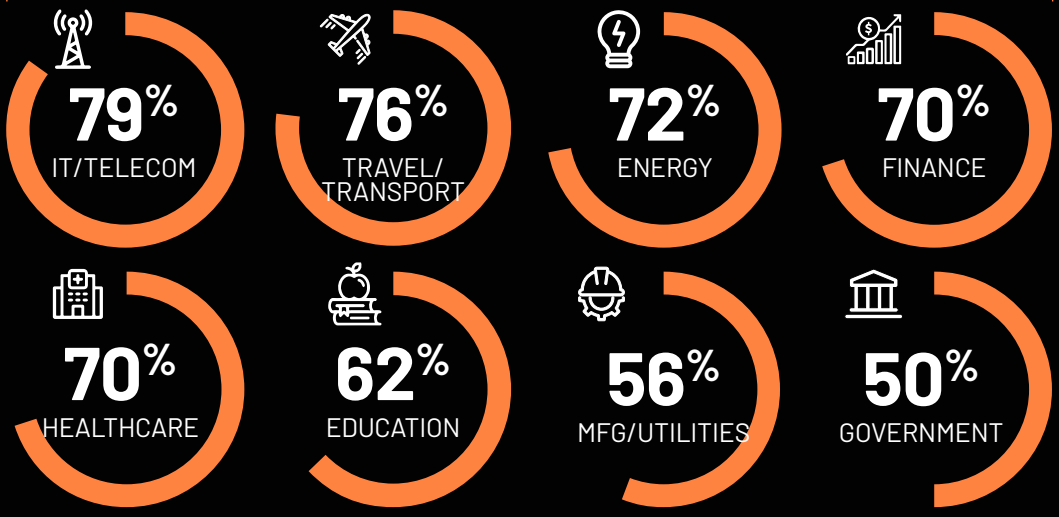


How often do you document and update cyber response runbooks and playbooks?

MONTHLY/QUARTERLY UPDATES

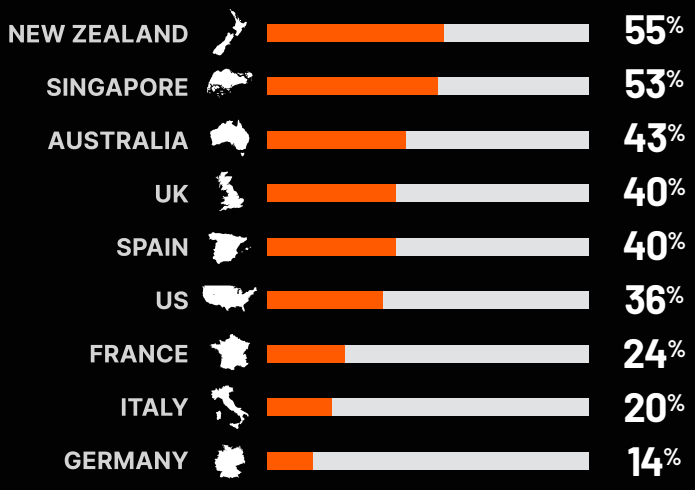


MONTHLY/QUARTERLY UPDATES

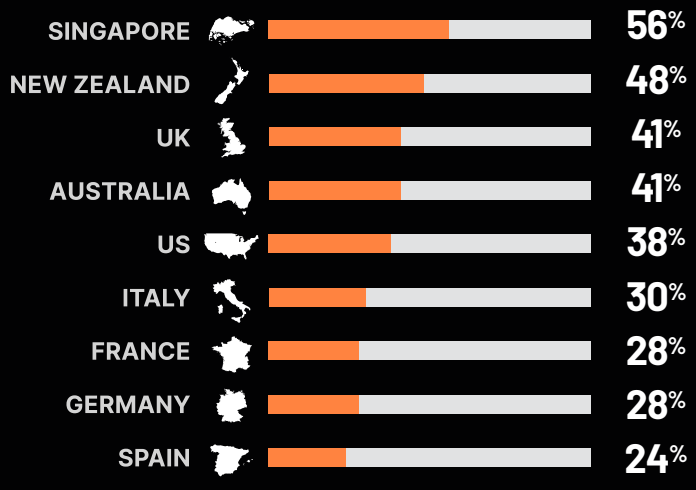


Who Attends Tabletop Crisis Response Exercises?

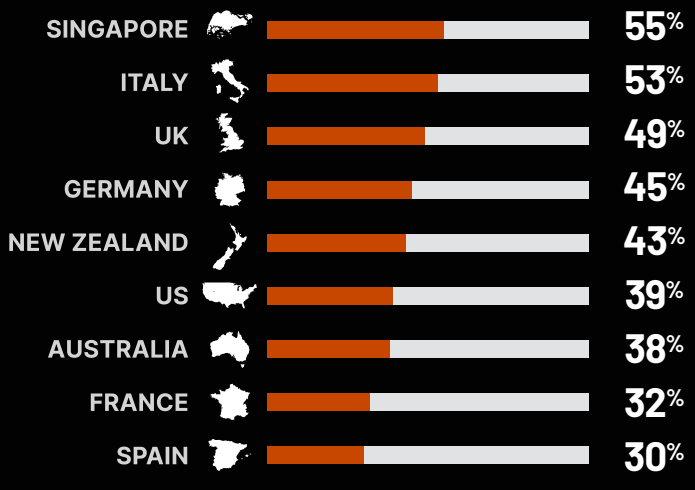
LEGAL, FINANCE, HR



BUSINESS CONTINUITY



DISASTER RECOVERY



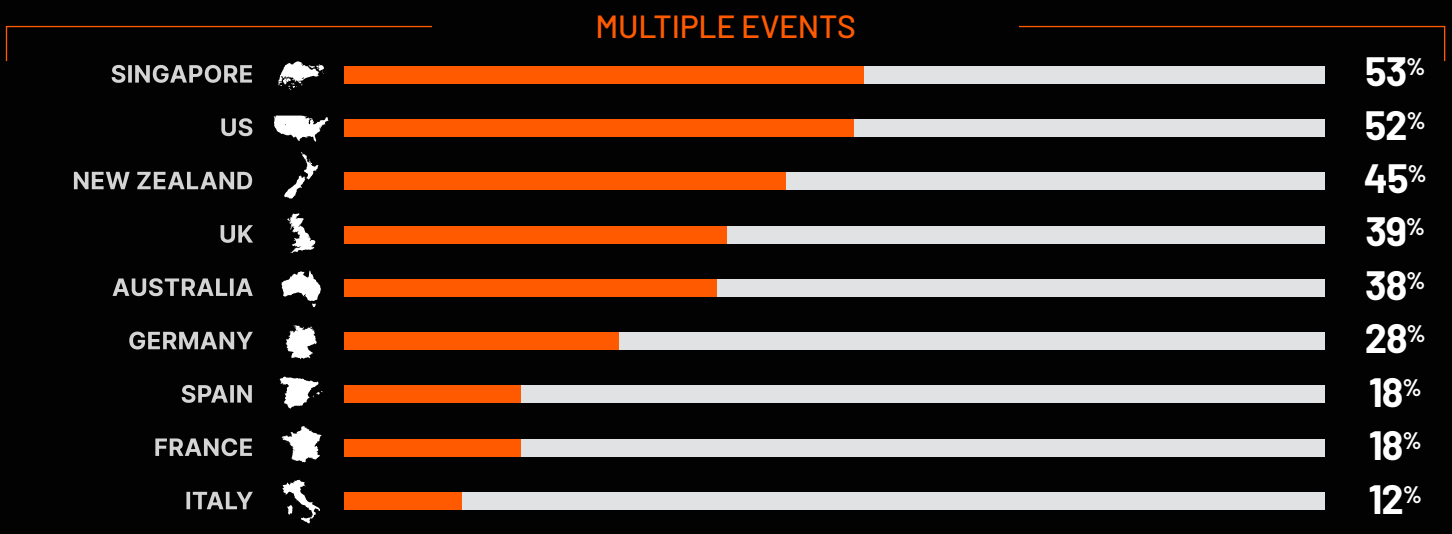
Only in Singapore do more than half of organizations include business stakeholders, business continuity teams, and disaster recovery teams — all vital participants in real-word cyber crises — in tabletop exercises.

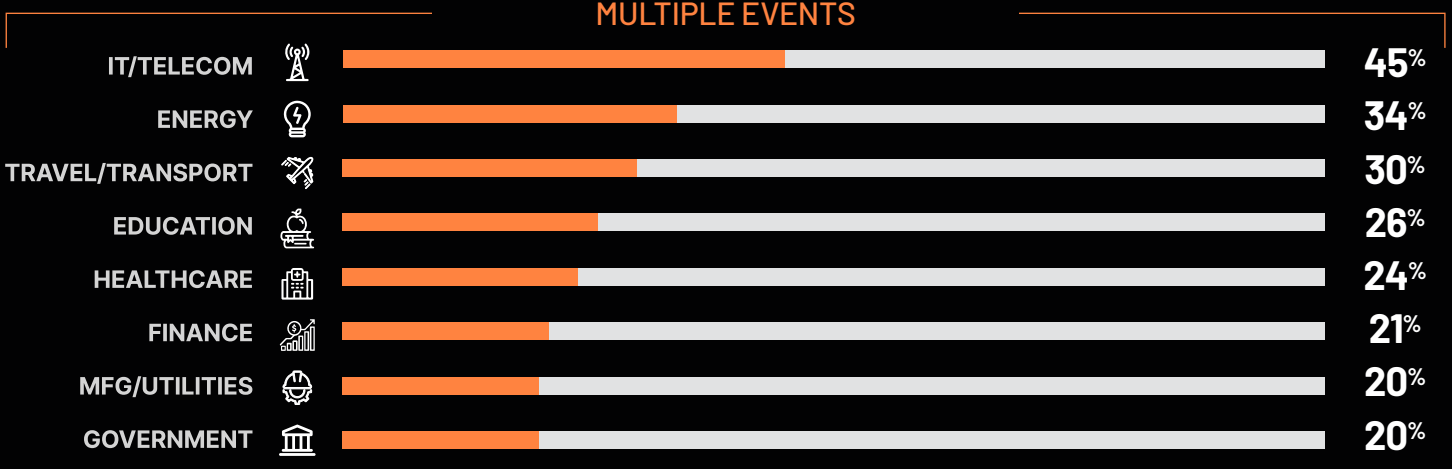
Can Your Plan Protect Business Resilience?

GLOBAL

71% Experienced at least one high-impact cyber event that halted critical business functions

36% Experienced multiple events



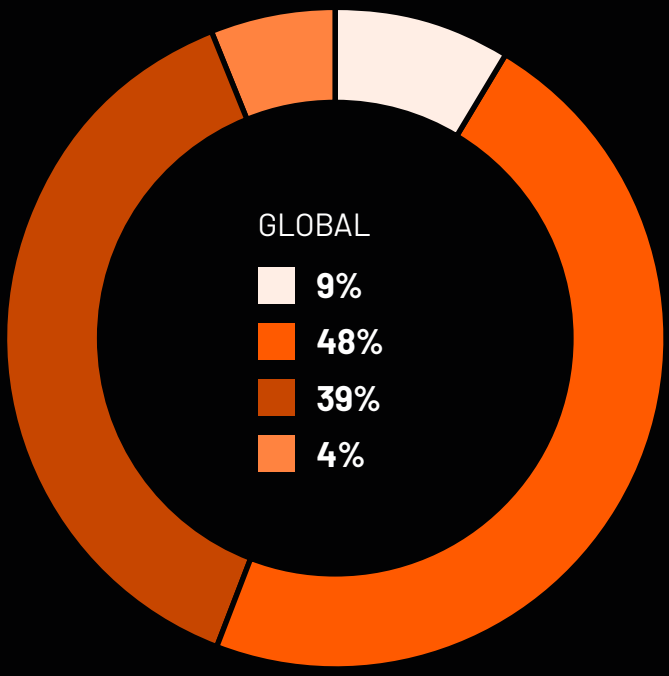


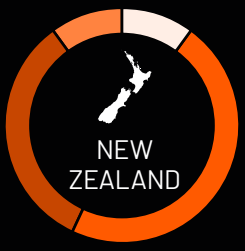
Only 51% of organizations in manufacturing/utilities reported high-impact events — the lowest among industries. Still, 82% needed to activate their enterprise crisis plans.

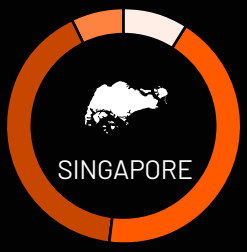
How many times has your enterprise crisis response team been activated to manage cyber incidents in the past year?

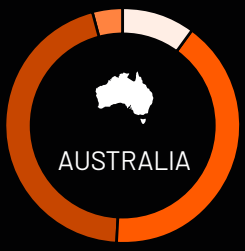
KEY

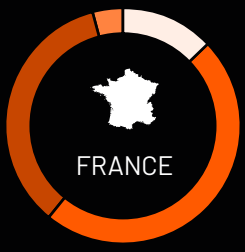
- 0 TIMES
- 1-4 TIMES
- 5-15 TIMES
- 16+ TIMES

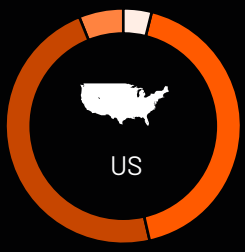


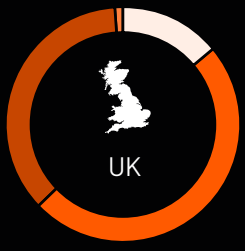


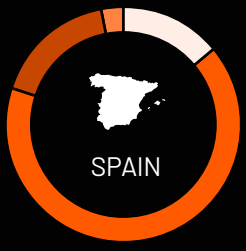












Methodology

To conduct this study, we partnered with experts at Censuswide, an international market research consultancy headquartered in London. In early 2025, Censuswide surveyed 1,000 organizations across the US, UK, France, Germany, Italy, Spain, Australia, New Zealand, and Singapore. Statistics in this study are reported as averages of responses from all surveyed countries or industries, based on their experience over the past 12 months.

How to cite information in this report

The data in this report are provided as an information source for the cybersecurity community and the organizations it serves. Semperis encourages you to share our findings. To cite statistics or insights, reference **Semperis' The State of Enterprise Cyber Crisis Readiness** report and link to the full report, which is downloadable at https://ready1.com.

To interview Semperis experts, contact Bill Keeler at billk@semperis.com. Lastly, we'd love to hear your questions or thoughts on the topic of ransomware and resilience. Find Semperis and Ready1 on LinkedIn.

About 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: https://ready1.com.

About Semperis

Semperis protects critical enterprise identity services for security teams charged with defending hybrid and multi-cloud environments from cyberattacks, data breaches, and operational errors. Purpose-built for securing hybrid identity environments — including Active Directory, Entra ID, and Okta — Semperis' AI-powered technology protects over 100 million identities from cyberattacks, data breaches, and operational errors.

Learn more: https://www.semperis.com.

ready1
powered by semperis

+1-703-918-4884 | info@semperis.com | www.semperis.com
5 Marine View Plaza, Suite 102, Hoboken, NJ 07030