RISK-READY OR RISK-EXPOSED

COHESITY

The Cyber Resilience Divide

Cyberattacks are no longer isolated events but an enduring feature of our digital world. Each day brings a new reminder as hospitals, government agencies, and global enterprises fall victim. No organization is immune, and the growing frequency and sophistication of threats have led to a surge in material cyberattacks that cause measurable financial, operational, and reputational damage.

A SURVEY OF 3,200 IT AND SECURITY OPERATIONS DECISION MAKERS ACROSS 11 COUNTRIES REVEALS THE REALITY.

76%
of organizations have faced a material cyberattack.

54%
were hit in the past 12 months.

1 IN 4
have been attacked multiple times.

THE DAMAGE RUNS DEEP AND **COSTS ADD UP FAST.**

87% Lost revenue

42% Lost customers

70% Of publicly listed organizations had to revise their financial guidance

92% Faced legal or regulatory consequences

82% Paid a ransom in the past 12 months

EVEN WITH THE EVIDENCE IN PLAIN SIGHT, MANY ORGANIZATIONS OVERESTIMATE THEIR RESILIENCE.

47%
have complete confidence in their cyber resilience strategy

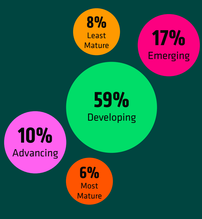
MOST STILL PRIORITIZE PREVENTION AND DETECTION OVER THE EQUALLY CRITICAL FUNCTIONS OF RESPONSE AND RECOVERY.

Order based on the NIST cybersecurity framework.
Box size shows highest to lowest proportion of cyber resilience investments.

#2	#1	#3	#4	#5
Identify	Protect	Detect	Respond	Recover

CONFIDENCE AND SPENDING PATTERNS **TELL ONLY PART OF THE STORY**

True resilience depends on the practices and capabilities that back them up. When assessed against real-world performance criteria, only 6% of organizations demonstrate maturity across five essential areas: **data protection**, **data recovery**, **threat detection and investigation**, **application resilience**, and **data risk optimization**.



For the most cyber resilient organizations, resilience is systematic and comprehensive. Among other best practices, they ensure sensitive data is backed up globally, multifactor authentication and admin controls are enforced, threat intelligence is maximized, recovery is secured through remediation, and compliance safeguards are consistently met.

YET EVEN THESE ELITE FEW KNOW THAT MATURITY ISN'T STATIC.

62%
Acknowledge their resilience strategies still have room to grow

That awareness is driving the next evolution – powered by automation and AI. As threats become faster and more complex, automation is key to accelerating detection, streamlining response, and strengthening recovery.

59%

say better automation across detection, response, and recovery is one of the top lessons learned following the cyberattack

37%

believe AI will play a central role in how they detect and respond to threats including making some autonomous decisions

99%

plan to use AI to support data security operations by 2026

ARE YOU RISK READY?

- **Download the full report** for detailed findings.
- **Book a Ransomware Resilience Workshop**
- Get our **"Five Steps to Cyber Resilience"** eBook to start advancing your maturity today.

Vanson Bourne surveyed 3,200 IT and security leaders from organizations with 1,000 or more employees in 2025, covering the North American, Asia-Pacific, European and Latin American regions.

COHESITY VansonBourne

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054
620001I-001-EN 11-2025