COHESITY

GLOBAL CYBER RESILIENCE REPORT

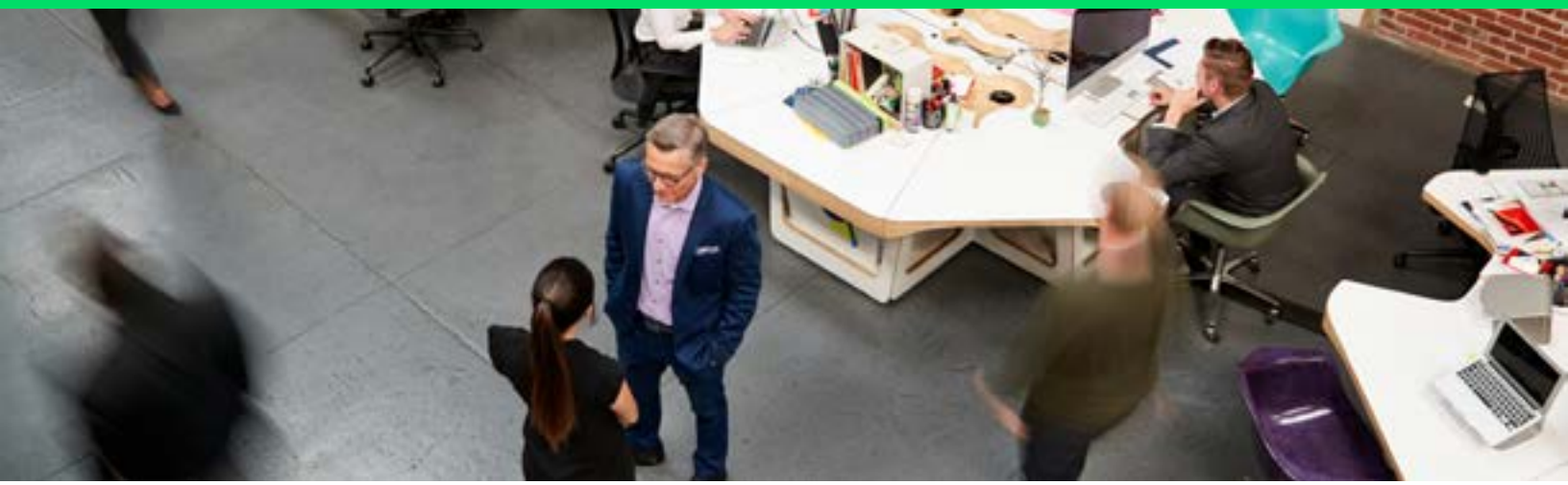
Risk-Ready vs. Risk-Exposed: The Cyber Resilience Divide

NOVEMBER 2025

Everyone talks about detecting and preventing cyberattacks, yet the headlines tell a different story. Prevention and detection alone aren't enough. Even the world's most sophisticated enterprises are suffering crippling disruptions that ripple from IT to the boardroom—and beyond.

To understand why, and what separates resilient organizations from those still struggling, Cohesity drew on the insights of 3,200 IT and Security Operations decision-makers worldwide. The findings reveal a widening resilience divide between risk-ready organizations that can recover quickly and confidently, and their risk-exposed peers that remain vulnerable to prolonged disruption and downstream damage.

Our research examines the real-world impacts of material cyberattacks, how organizations self-assessed their cyber resilience against best practices, and the steps they took to detect, respond to, and recover from these incidents. It also highlights what organizations are learning from experience, and how they are turning to AI and automation to accelerate resilience and close the divide.



MATERIAL CYBERATTACKS: **THE NEW REALITY OF MODERN BUSINESS**

Cyber incidents are not created equal. Many organizations manage routine phishing attempts, malware probes, or minor outages on a near-daily basis. But material cyberattacks are different. These are the attacks that halt operations, trigger financial losses for both the organization and its customers, damage reputations, and draw scrutiny from boards, regulators, and stakeholders alike.

THESE HIGH-IMPACT ATTACKS ARE NO LONGER ISOLATED INCIDENTS.

76%

have experienced at least one material cyberattack.

54%

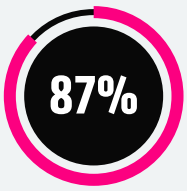
experienced an attack within the past 12 months.

26%

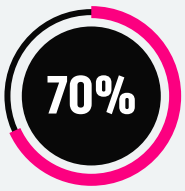
endured multiple attacks during that same period.

THE ACTUAL COST OF MATERIAL CYBERATTACKS

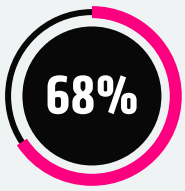
FINANCIAL AND REGULATORY PRESSURES ALSO ECHOED ACROSS THE ORGANIZATIONS WE SURVEYED:



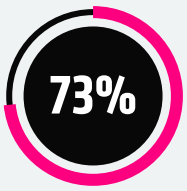
reported revenue loss



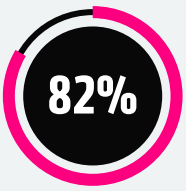
of publicly listed companies reported adjusting financial guidance



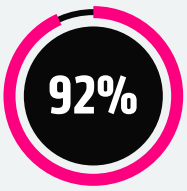
said they observed an impact on stock price



of privately held firms diverted budgets from growth initiatives



paid a ransom averaging $1.3M per incident



faced legal or regulatory consequences, including monetary fines (46%) and lawsuits or class-action litigation (35%)

INTERPRETING THE NUMBERS

While only a small number of public companies have formally disclosed changes to earnings guidance following a cyber incident, the high percentages seen in this research indicate that respondents view material cyberattacks as producing broader financial strain and operational consequences than what public filings typically capture. This disconnect between market perception and organizational reality is likely influenced by limited disclosure requirements, narrow investor definitions of materiality, and the underestimation of intangible losses such as brand trust, customer churn, and productivity.

CONFIDENCE IN THE FACE OF CONSEQUENCE

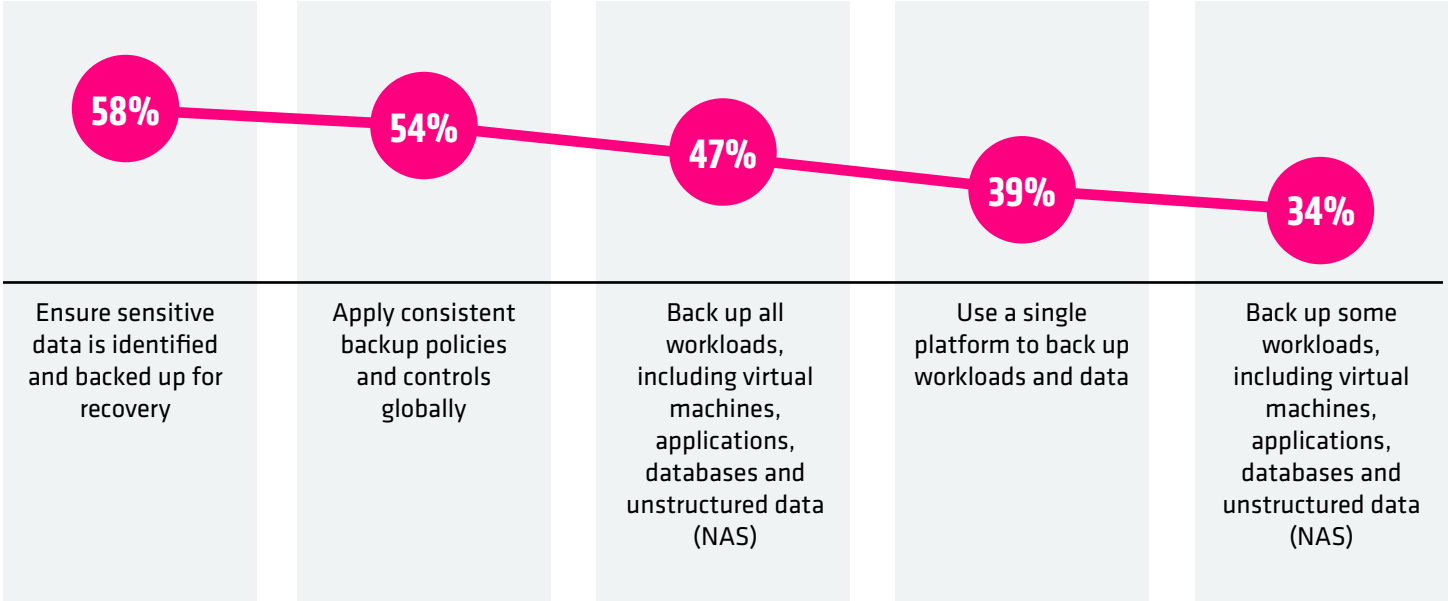
Given the scale of financial and operational fallout revealed in our research, one might expect widespread concern about organizational resilience. Nearly half of respondents (47%) expressed complete confidence that their cyber-resilience strategy could withstand today's threats. This level of confidence stands in sharp contrast to the significant material impacts many of these same organizations have sustained.

WHAT ORGANIZATIONS ARE (AND AREN'T) DOING

We wanted to look beneath the surface and discover where resilience gaps exist. To do that, we asked respondents to describe their approach to some of the key practices and capabilities associated with five core dimensions of cyber resilience: **data protection**, **data recovery**, **threat detection and investigation**, **application resilience**, and **data risk posture optimization**.

DATA PROTECTION REMAINS FRAGMENTED ACROSS HYBRID AND MULTICLOUD ENVIRONMENTS

What does your organization do to protect all data across hybrid and/or multi-cloud environments?



A majority of organizations back up sensitive data and enforce basic policies, but data protection remains fragmented. Less than half are consistent across all workloads and just 39% rely on a single platform. This patchwork approach compromises visibility, exposes data, and complicates response and recovery efforts. Mature cyber resilience depends on unifying backup and recovery within one intelligent platform secured by Zero Trust principles.

MOST CANNOT ENSURE DATA IS TRULY RECOVERABLE POST ATTACK

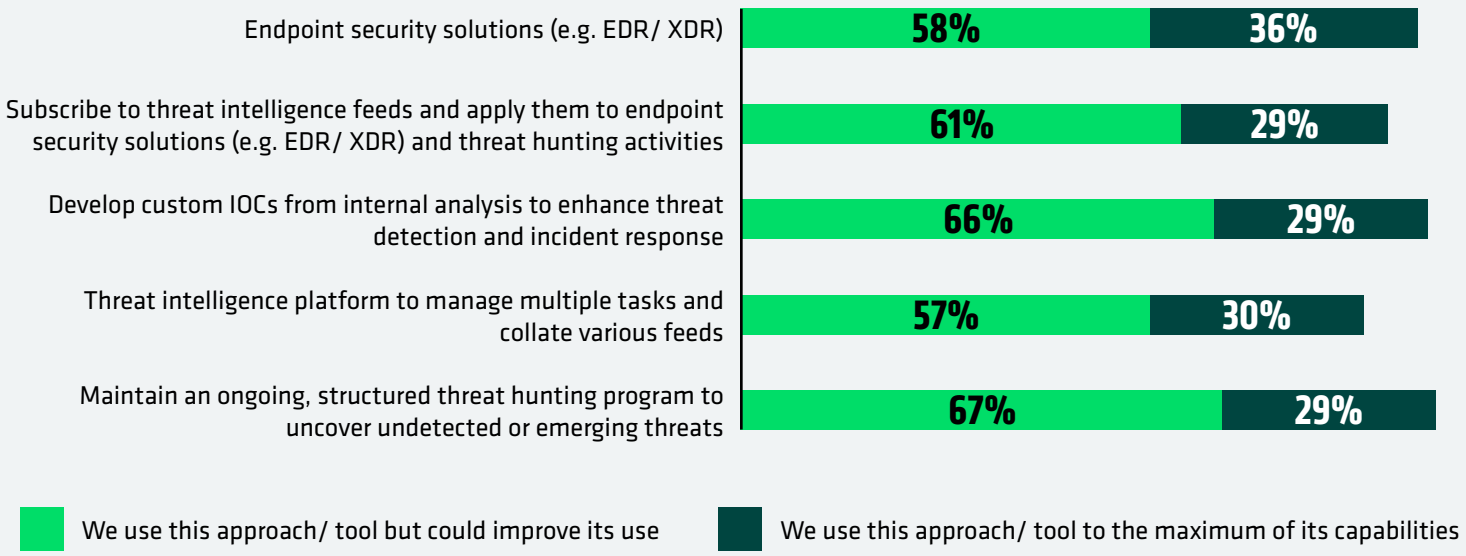
What does your organization do to ensure that its data is always recoverable?

59%	Require additional authorization on high-risk admin tasks associated with backup and recovery solutions
54%	Have multi-factor authentication on their backup solution
48%	Follow the "3-2-1 backup rule" (three copies of data, stored on two different media types, with one copy kept off-site)
44%	Protect critical data with immutability
41%	Least privilege access rights on backed up workloads

Many organizations have hardened access controls around their backup environments. Nearly six in 10 now require extra admin authorization, and slightly over half enforce multifactor authentication. Yet not all can ensure that data is truly recoverable post attack. Fewer than half follow the 3-2-1 backup rule or use immutability. Mature cyber resilience demands verified, isolated, and tamper-proof recovery copies.

THREAT DETECTION AND INVESTIGATION TOOLS ARE UNDERUTILIZED

To what extent does your organization use each of the following methods or tools to detect and investigate threats?



Threat detection and investigation tools are widely adopted but not fully utilized. Most organizations use endpoint security, threat intelligence feeds, and structured threat hunting programs, yet only about a third leverage these tools to their full potential. Mature cyber resilience depends on integrating them into a continuous intelligence loop that improves visibility, detection, and response.

ORGANIZATIONS ARE VULNERABLE TO REINFECTION

What does/ would your organization do to ensure application resilience against cyberattacks?

59% Identify and remediate security control gaps before restoring systems to production

58% Conduct annual end-to-end simulated rehearsals including a cross functional team of technical, legal, strategic, executive and communications stakeholders

55% Use online, vaulted repository of critical systems and information to support incident response and recovery

49% Use an isolated environment for incident investigation, remediation and secure recovery

37% Immutability for all backup data

Organizations are advancing their approach to application resilience, but gaps remain. Most conduct recovery rehearsals and address control weaknesses before restoring systems, but few maintain isolated or immutable environments, leaving recovery vulnerable to reinfection or data loss. Mature cyber resilience pairs preparation with secure, verifiable recovery zones.

BACKUPS ARE OFTEN NOT PRIORITIZED

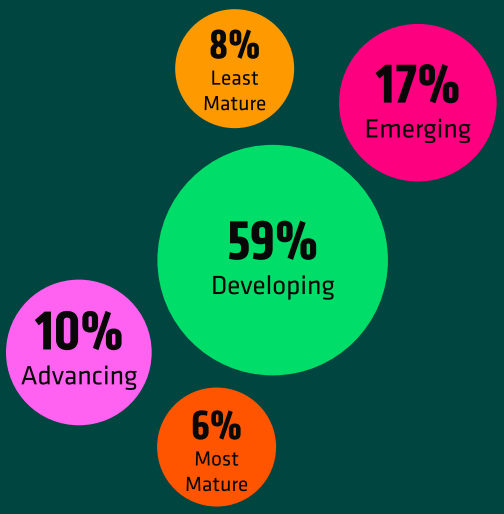
How does your organization use data discovery and classification approaches/ tools to minimize data risk exposure across its entire data estate?

Organizations are using data discovery and classification more strategically across compliance, response, and recovery. Most address privacy violations and utilize classification to guide obligations during an attack, but fewer assess materiality or prioritize backups based on risk. Mature cyber resilience transforms classification into a systematic approach for optimizing data risk posture, informing protection, response, and recovery.

A CLEARER PICTURE OF RESILIENCE MATURITY

When scored collectively, respondents' answers served as a high-level barometer of cyber resilience maturity, revealing clear patterns in how organizations are building – or struggling to build – resilience in practice. While the majority fall into the developing stage, only 6% demonstrate most mature, integrated capabilities that define risk-ready organizations.

THE CYBER RESILIENCE MATURITY CURVE



Least Mature (8%): Backups, policies, and security safeguards are largely absent or inconsistent. MFA and admin controls are rarely enforced, recovery often lacks isolation, and compliance or materiality assessments are typically overlooked.

Emerging (17%): Some resilience practices are in place, but inconsistently. Organizations may back up sensitive data, apply global policies, or use MFA, but rarely in combination. Threat intelligence and compliance efforts exist yet remain immature and fragmented.

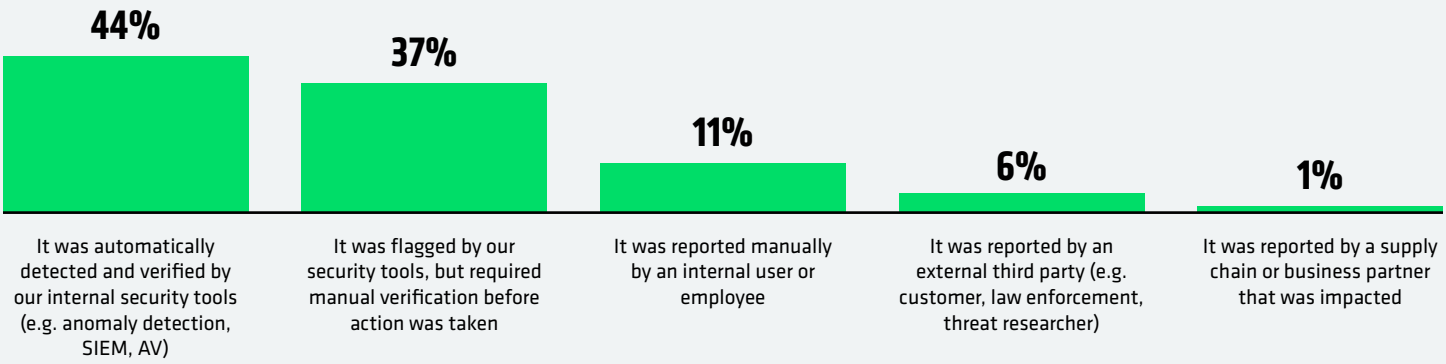
Developing (59%): Core practices such as backups, admin controls, and threat intelligence are more common, though still uneven. Recovery environments, compliance checks, and security gap remediation are applied sporadically, leaving resilience efforts partially effective.

Advancing (10%): Most key practices are consistently enforced, including global backup policies, admin approvals, and remediation before recovery. Threat intelligence is used but not fully optimized, and some gaps remain around isolated recovery and full compliance coverage.

Most Mature (6%): Resilience is systemic and comprehensive. Sensitive data is backed up globally, MFA and admin controls are standard, threat intelligence is maximized, recovery is secured through remediation, and compliance safeguards are consistently met.

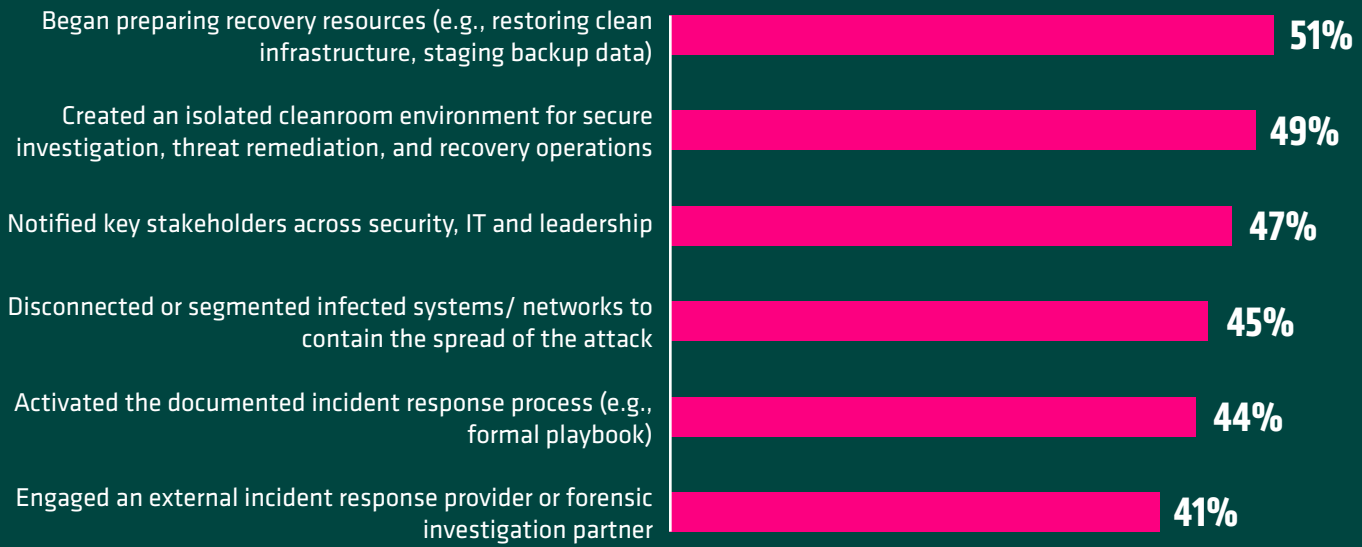
RESILIENCE UNDER FIRE

HOW TEAMS IDENTIFIED THE ATTACK



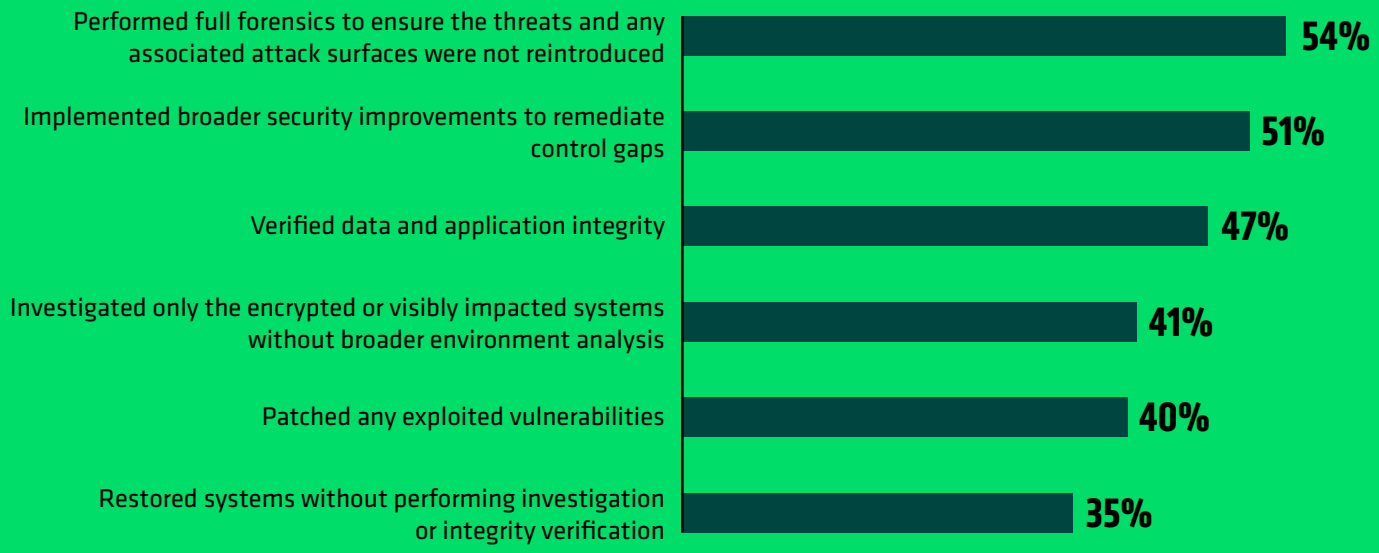
In the event of a cyberattack, most organizations first detect them internally. Nearly half (44%) said incidents were automatically identified and verified by their own security tools. Another 37% manually verified the issue after alerts were triggered. Only a small fraction relied on employee or third-party reports, showing that detection is mainly internal, but still heavily dependent on manual confirmation.

ACTIONS TEAMS TOOK AFTER CONFIRMING THE ATTACK



Once they confirmed the attacks, organizations quickly prepared for recovery. Just over half began restoring clean infrastructure or staging backup data, and nearly as many established isolated cleanroom environments for secure investigation and remediation. Roughly half also notified stakeholders and contained infected systems, but fewer activated formal playbooks or engaged external experts, signaling that response actions remain uneven across critical steps.

STEPS TAKEN BEFORE BRINGING SYSTEMS AND DATA BACK ONLINE



Before bringing systems back online, most performed at least some level of forensic and remediation work. Over half of organizations conducted full forensics to ensure they eradicated all threats, and 51% strengthened their controls more broadly. Yet, fewer verified data integrity checks or patched vulnerabilities, and more than a third of of systems were restored without full validation–leaving room for reinfection risk.

CHALLENGES TEAMS FACED DURING THE ATTACK

Teams also reported significant challenges throughout the process. Many struggled to communicate or coordinate due to critical systems being offline. Others faced pressure from leadership to restore operations before remediation was complete. Security tool evasion, reinfection, and limited access to clean recovery points compounded these difficulties, highlighting how operational disruption and organizational pressure can undermine even well-prepared response and recovery efforts.

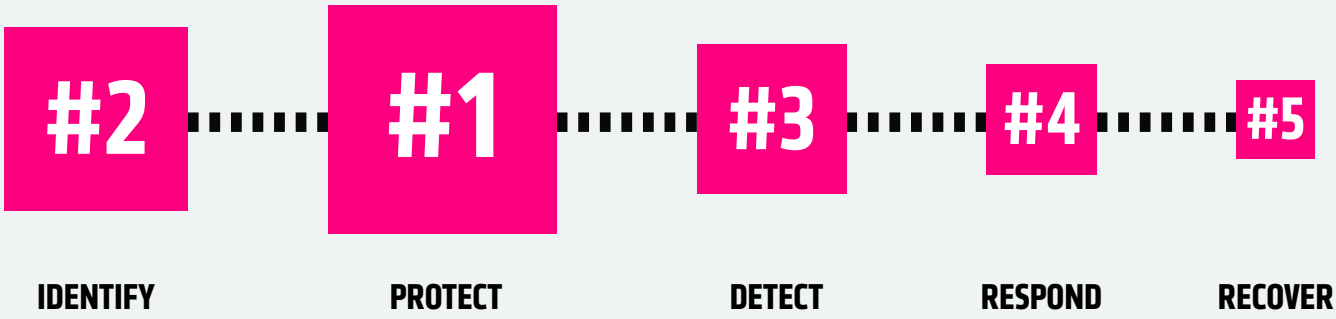
WHERE RESILIENCE INVESTMENT STILL FALLS SHORT

The findings make clear that even well-prepared organizations encounter significant challenges once an attack is underway. Detection and containment capabilities are improving, but gaps in coordinated response, clean recovery, and post-incident assurance persist.

These patterns mirror how organizations are allocating their cyber resilience budgets today. We asked respondents how they proportion spending across the five core functions of the NIST Cybersecurity Framework—Identify, Protect, Detect, Respond, and Recover. Most continue to invest heavily in prevention, protection, and detection, while comparatively less funding supports response and verified recovery. The result is a maturity curve still weighted toward defense rather than restoration, highlighting an untapped opportunity to strengthen resilience where it matters most: after the attack.

NIST CYBERSECURITY FRAMEWORK.

Box size shows highest to lowest proportion of cyber resilience investments



AI AND AUTOMATION EMERGE AS RESILIENCE MULTIPLIERS

The results also show that organizations view AI as a powerful enabler of cyber resilience, particularly in improving detection speed and response precision. Nearly all respondents rated tools such as anomaly detection, user behavior analytics, and AI-driven threat investigation and response as effective in strengthening their security posture.

Even newer GenAI-based assistants, capable of natural language threat queries and contextual analysis, are gaining traction as a way to simplify and accelerate decision-making. Fifty-nine percent of organizations said one of their biggest lessons learned after a cyberattack was the need for greater automation across detection, response, and recovery. This reflects the growing demand for integrated automation and orchestration platforms, where AI acts as a force multiplier, driving greater efficiency, consistency, and effectiveness across these processes.

When looking ahead, most organizations expect AI to play an increasingly strategic role in cyber defense by the end of 2026. Over half (52%) anticipate AI will support human decision-making, enhancing analysis and recommendations, with humans remaining in control of final actions. Another 37% expect AI to become central to detection and response, even making some autonomous decisions. This signals a clear trajectory: AI is evolving from an assistant to an operational cornerstone of cyber resilience, poised to enhance speed, precision, and confidence across detection, response, and recovery.

THE FUTURE OF RESILIENCE STARTS NOW

While organizations are making measurable progress in cyber resilience, many still have room to improve their response, recovery and validation of readiness after an attack. Cyber resilience represents a massive competitive advantage. The future belongs to organizations that invest in the people, products, and processes to recover faster, maintain customer trust, and keep business moving when others can't. When disruption is virtually inevitable, resilience isn't just protection; it's performance.

Build resilience before crisis strikes:

- Book a Ransomware Resilience Workshop.
- Level up with a five-step cyber resilience action plan.
- Learn about Cohesity's cyber resilience solutions.

METHODOLOGY

COHESITY

Cohesity commissioned Vanson Bourne to survey 3,200 IT and Security decision-makers in September 2025, forming the basis of these findings. Respondents represent organizations in the US (500), Brazil (200), UK (400), Germany (400), France (400), UAE/Saudi (100), Australia (200), South Korea (200), Japan (400), India (200) and Singapore (200). The organizations had 1,000 or more employees and came from a range of public and private sectors, with a focus on financial services, public sector, and healthcare.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000049-001 EN 11-2025