COHESITY

CYBER RESILIENCE REPORT

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

FEBRUARY 2026

Everyone talks about detecting and preventing cyberattacks, yet the headlines tell a different story. Prevention and detection alone are no longer enough. Even the most advanced organizations are suffering crippling disruptions that ripple from IT operations to the boardroom—and beyond.

To understand why, and what separates resilient organizations from those still struggling, Cohesity surveyed 3,200 IT and Security Operations decision-makers across 11 countries. Among those were 371 participants from healthcare organizations. Their responses reveal a widening resilience divide between risk-ready healthcare organizations that can recover quickly and confidently, and their risk-exposed peers that remain vulnerable to prolonged disruption and downstream financial damage.

Our research examines the real-world impacts of material cyberattacks, how healthcare 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 they learned, and how they're 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 healthcare organizations manage routine phishing attempts, malware probes, or system outages on a near-daily basis. But material cyberattacks are different. Our survey defined a material cyberattack as an incident that caused measurable financial, reputational, operational, or customer churn impact.

THESE HIGH-IMPACT ATTACKS ARE NO LONGER ISOLATED EVENTS FOR HEALTHCARE ORGANIZATIONS.

85%

of respondents have experienced at least one material cyberattack

66%

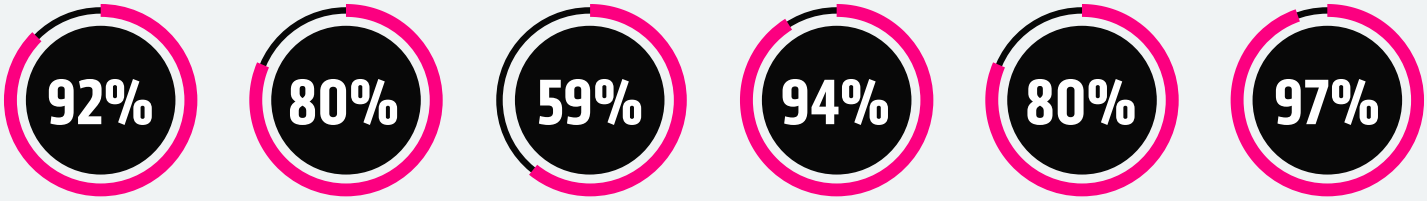
experienced one within the past 12 months

35%

endured multiple incidents during the 12-month period

THE ACTUAL COST OF MATERIAL CYBERATTACKS

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



reported revenue loss

of publicly listed healthcare organizations reported revising financial guidance[1]

lost customers or patients

paid a ransom—averaging USD 1.3 million per incident

of privately held healthcare organizations reallocated budget away from growth initiatives

faced legal or regulatory consequences, including regulatory fines (54%) and lawsuits or class action litigation (39%)

[1]While relatively few public companies have formally disclosed earnings revisions after a cyber incident, these findings suggest that the financial and operational effects extend well beyond what public filings reveal.

CONFIDENCE IN THE FACE OF CONSEQUENCE

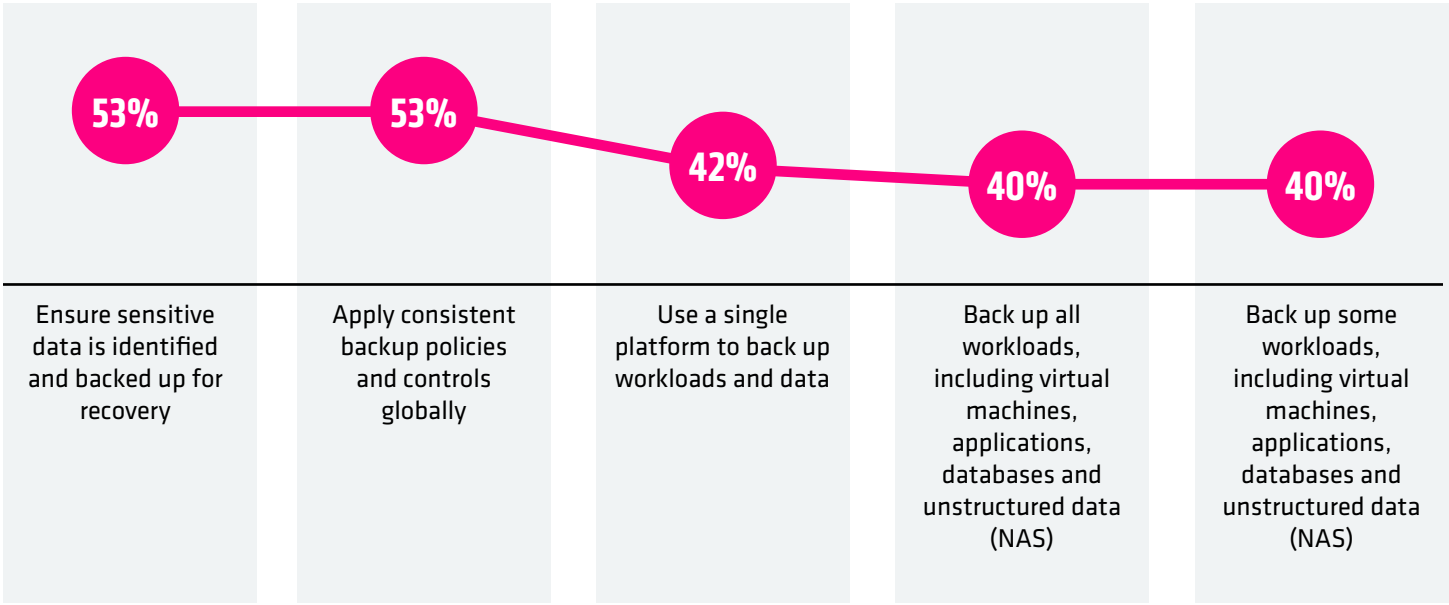
Given the scale of financial and operational fallout revealed in our research, one might expect widespread concern about organizational resilience. However, nearly half of respondents (49%) expressed complete confidence that their cyber-resilience strategy could withstand today's threats. This level 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?



Just over half of healthcare organizations ensure sensitive data is identified and backed up for recovery. The same percentage applies consistent backup policies globally. However, fewer than half back up all workloads or rely on a single platform. A little more than a third back up only selected workloads. This fragmentation limits visibility and consistency across environments. Mature cyber resilience depends on unifying backup and recovery within a single intelligent platform secured by Zero Trust principles.

DATA RECOVERABILITY MEASURES ARE COMMON BUT MATURITY VARIES

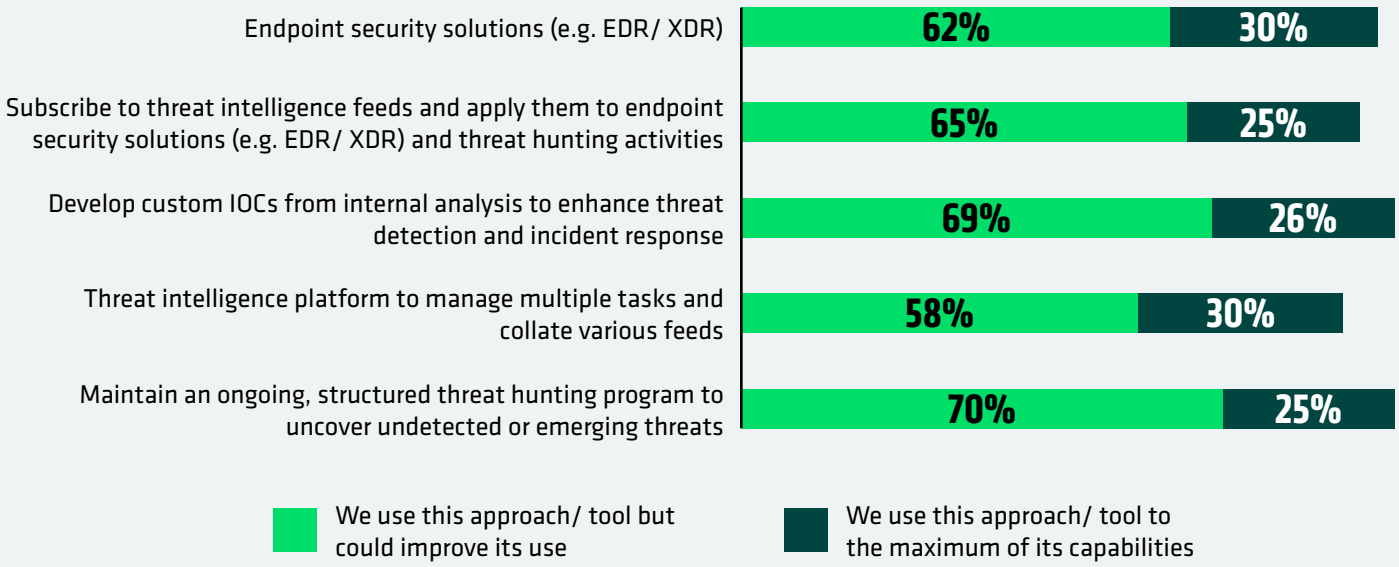
What does your organization do to ensure that its data is always recoverable?

60%	Require additional authorization on high-risk admin tasks associated with backup and recovery solutions
48%	Have multi-factor authentication on their backup solution
44%	Follow the "3-2-1 backup rule" (three copies of data, stored on two different media types, with one copy kept off-site)
42%	Protect critical data with immutability
35%	Least privilege access rights on backed up workloads

Many healthcare organizations have strengthened access controls around backup environments, with six in 10 requiring additional admin authorization for high-risk tasks. Fewer than half enforce multifactor authentication, follow the 3-2-1 backup rule, or protect critical data with immutability. Only about a third apply least-privilege access rights. These gaps make full recovery less certain. Mature cyber resilience depends on 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 deployed but often underutilized. Most healthcare organizations use endpoint security, threat intelligence feeds, and structured threat hunting programs, yet only a minority leverages these tools to their full potential. Optimization of advanced capabilities such as custom indicators of compromise (IOCs) and threat intelligence platforms remains particularly limited. Mature cyber resilience depends on integrating these tools 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?

56% Conduct annual end-to-end simulated rehearsals including a cross functional team of technical, legal, strategic, executive and communications stakeholders

54% Identify and remediate security control gaps before restoring systems to production

53% Use online, vaulted repository of critical systems and information to support incident response and recovery

36% Use an isolated environment for incident investigation, remediation and secure recovery

36% Immutability for all backup data

Healthcare organizations are advancing their approach to application resilience, but gaps remain. Over half identify security control gaps before restoring systems and conduct annual recovery rehearsals. A similar share maintains online, vaulted repositories to support response and recovery. Fewer use isolated environments for secure investigation and recovery or apply immutability across all backup data. These gaps leave recovery processes vulnerable to reinfection or data loss. Mature cyber resilience pairs preparation with secure, verifiable recovery zones.

DATA CLASSIFICATION GAINS TRACTION, BUT RISK-DRIVEN USE STILL EVOLVING

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

Use backup data classification to determine compliance obligations for impacted data

Identify and resolve backup privacy and security violations for compliance

Define and understand cyberattack materiality before an incident occurs

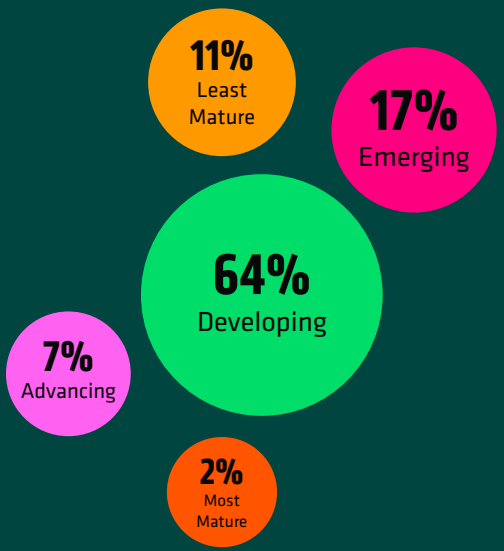
Identify and prioritise systems for backup

Healthcare organizations are using data discovery and classification more strategically across compliance, response, and recovery. Six in ten use classification to guide compliance during an attack while close to the same number addresses privacy and security violations. Slightly fewer define materiality before an incident or prioritize backups based on risk. These gaps suggest that risk-driven use of classification is still evolving. Mature cyber resilience transforms classification into a systematic approach that optimizes data risk posture and informs 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 healthcare organizations are building – or struggling to build – resilience in practice. While the majority fall into the developing stage, only 2% demonstrate the most mature, integrated capabilities that define risk-ready organizations.

THE CYBER RESILIENCE MATURITY CURVE



Least Mature (11%): 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.

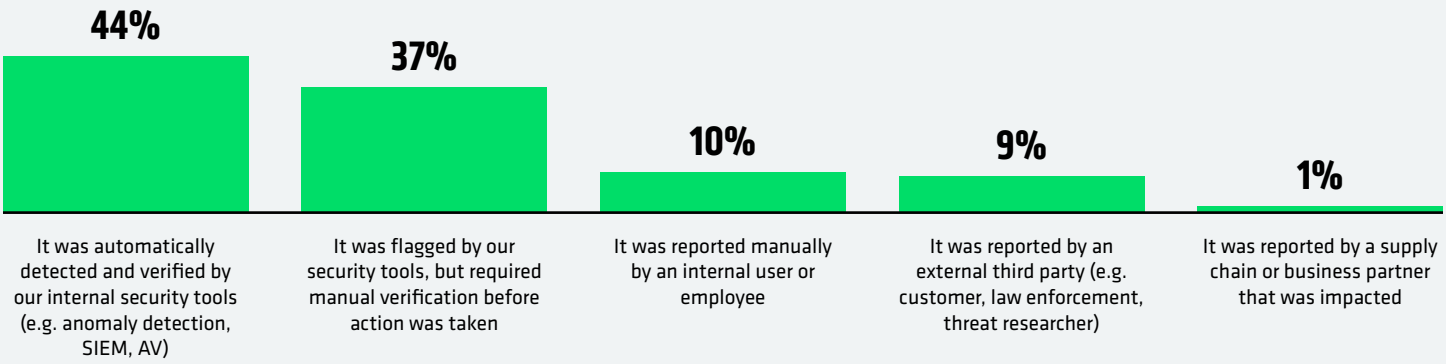
Developing (64%): Core practices such as backups, admin controls, and threat intelligence are more common, though still uneven. Recovery environments, compliance checks, and security gap remediation are applied sporadically, leaving resilience efforts partially effective.

Advancing (7%): 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 (2%): 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.

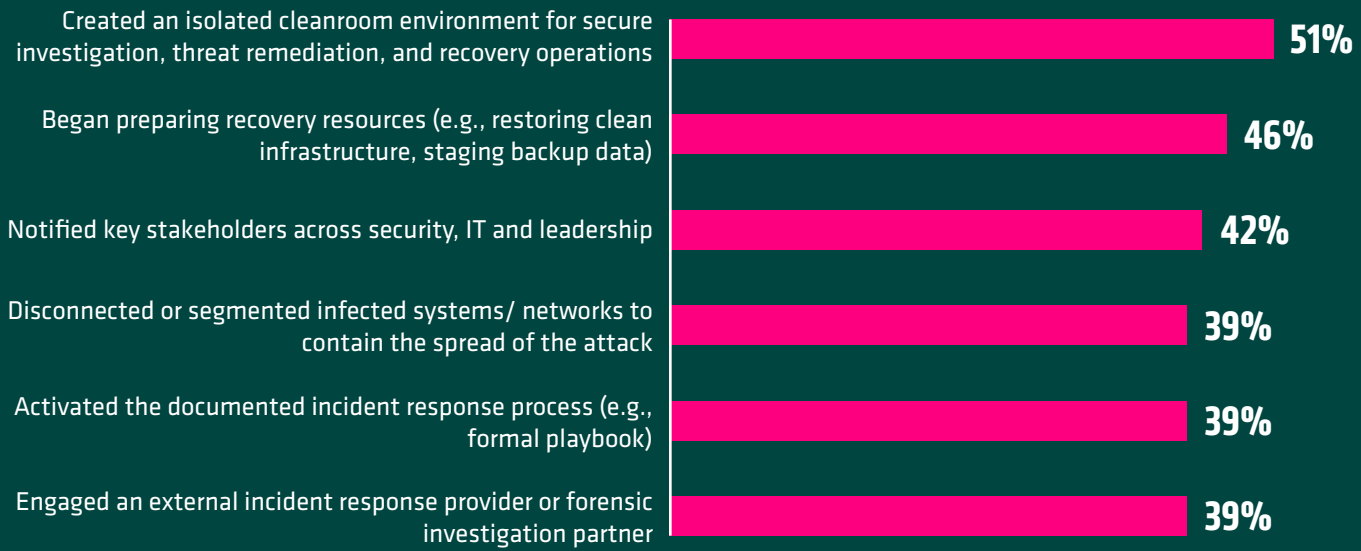
RESILIENCE UNDER FIRE

HOW TEAMS IDENTIFIED THE ATTACK



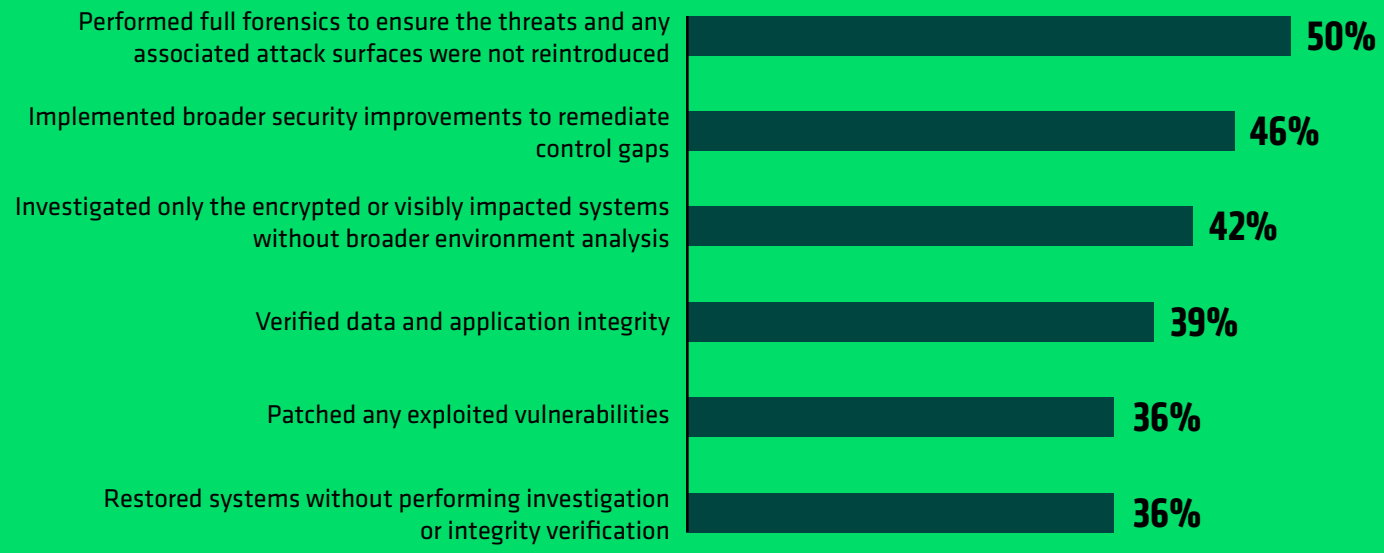
In the event of a cyberattack, nearly half of healthcare organizations said attacks were automatically identified and verified by their own security tools, while more than a third were flagged by tools, but required manual verification before action was taken. Alerts from third parties were much less frequent. Detection appears largely internal but still dependent on human confirmation.

ACTIONS TEAMS TOOK AFTER CONFIRMING THE ATTACK



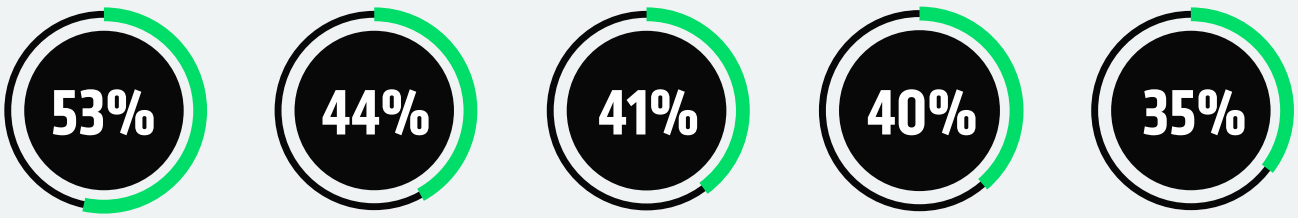
After confirming an attack, healthcare organizations took a range of actions to support recovery. Just under half began restoring clean infrastructure or staging backup data. Over half established isolated cleanroom environments for secure investigation and recovery. Around four in ten notified key stakeholders, contained infected systems, activated formal response playbooks, or engaged external incident response or forensic experts. These variations indicate that response actions are not yet fully standardized across critical steps.

STEPS TAKEN BEFORE BRINGING SYSTEMS AND DATA BACK ONLINE



Before bringing systems back online, healthcare organizations took a mix of forensic and remediation actions. Half performed full forensics while just under half implemented broader security improvements. Fewer verified data and application integrity, patched exploited vulnerabilities, or investigated beyond the visibly impacted systems. Over a third restored systems without full investigation or integrity verification, leaving openings for reinfection and residual risk.

CHALLENGES TEAMS FACED DURING THE ATTACK



Teams reported significant challenges throughout the process. Many struggled to communicate or coordinate while critical systems were offline. Nearly half faced pressure to restore operations before remediation was complete. Security tool evasion, reinfection, and lack of clean recovery points compounded difficulties, highlighting the need for stronger resilience measures.

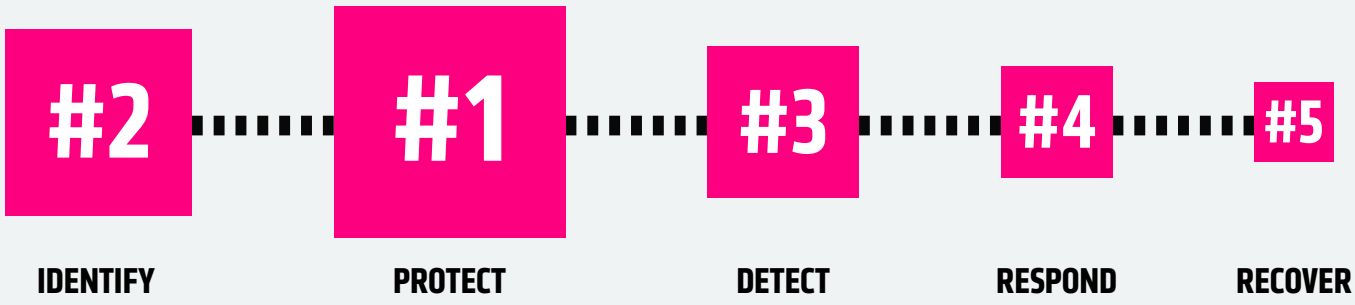
WHERE RESILIENCE INVESTMENT STILL FALLS SHORT

Even well-prepared healthcare organizations struggle to sustain resilience once an attack unfolds. As operational pressure mounts, coordination gaps, incomplete remediation, and reinfection risks expose how fragile recovery can be without unified processes and continuous assurance.

These patterns mirror how healthcare 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 healthcare 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. Sixty-one percent of healthcare organizations said one of the 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 expect AI to play an increasingly strategic role in cyber defense by the end of 2026. Fifty-four percent anticipate AI will support human decision-making, enhancing analysis and recommendations, with humans remaining in control of final actions. Thirty-seven percent 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 healthcare 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 for Healthcare

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 Arabia (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

2000072-001 EN 2-2026