COHESITY

INDIA CYBER RESILIENCE REPORT

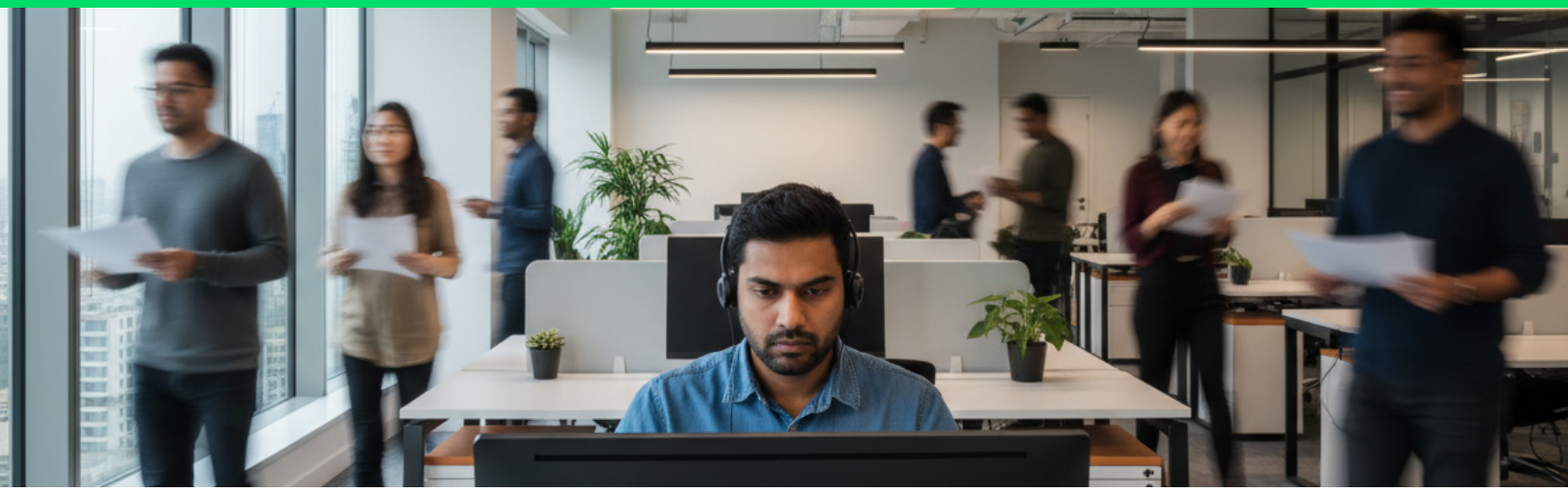
Risk-Ready vs. Risk-Exposed: The Cyber Resilience Divide In India

DECEMBER 2025

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 enterprises are suffering crippling disruptions that ripple from IT operations to the boardroom—and beyond.

To understand why, and what separates resilient organisations from those still struggling, Cohesity surveyed 200 IT and Security Operations decision-makers across India. The findings reveal a widening resilience divide between risk-ready organisations 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 Indian organisations 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 organisations manage routine phishing attempts, malware probes, or system outages on a near-daily basis. But material cyberattacks are different. These are the attacks that halt operations, trigger financial losses, damage reputations, and draw scrutiny from boards, auditors, and regulators such as the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), and the Indian Computer Emergency Response Team (CERT-In).

THESE HIGH-IMPACT ATTACKS ARE NO LONGER ISOLATED INCIDENTS.

78%

of Indian organisations have experienced at least one material cyberattack.

61%

experienced one within the past 12 months.

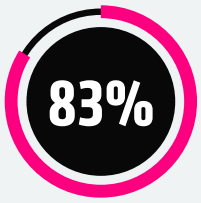
31%

endured multiple incidents during the 12-month period.

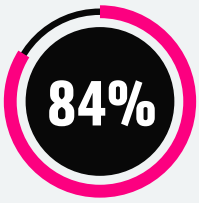
THE ACTUAL COST OF MATERIAL CYBERATTACKS

FINANCIAL AND REGULATORY PRESSURES ALSO ECHOED ACROSS INDIAN ORGANISATIONS WE SURVEYED:

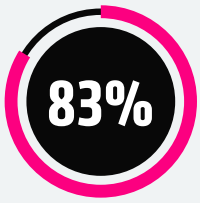
reported revenue loss



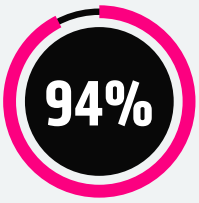
of publicly listed Indian companies reported revising financial guidance[1]



of privately held Indian firms diverted budgets from growth initiatives



paid a ransom—averaging USD 1.41 million per incident



faced legal or regulatory consequences, including financial penalties (46%) and regulatory or collective legal actions (26%)

[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

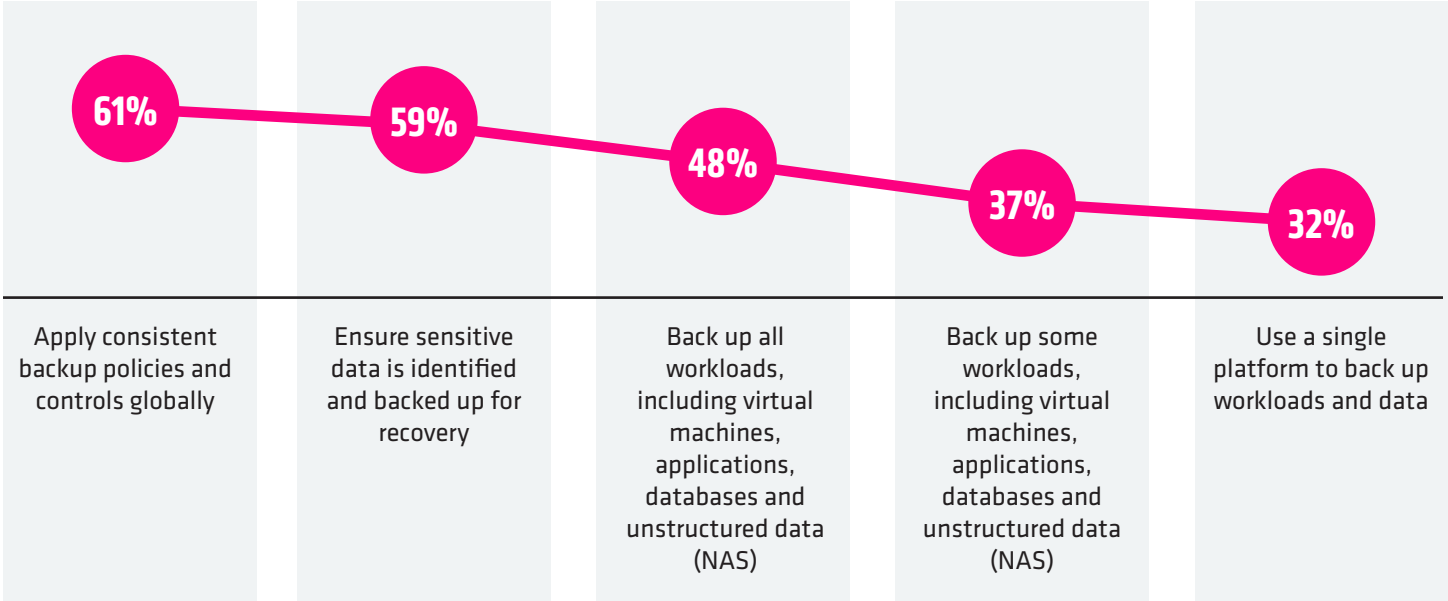
Given the scale of financial and operational fallout revealed in our research, one might expect widespread concern about organisational resilience. Nearly half of respondents (49%) expressed complete confidence that their cyber-resilience strategy could withstand today's threats. This level of confidence stands in sharp contrast to the significant material impacts many of these same organisations 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 optimisation.**

DATA PROTECTION REMAINS FRAGMENTED ACROSS HYBRID AND MULTICLOUD ENVIRONMENTS

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



A majority of Indian organisations ensure sensitive data is identified and backed up for recovery, and six in ten apply consistent backup policies and controls globally. Yet data protection remains fragmented. Fewer than half back up all workloads, including virtual machines and unstructured data, and only a third use a single platform, while 37% back up only selected workloads. This patchwork approach limits visibility, increases exposure, and complicates recovery. Mature cyber resilience depends on unifying backup and recovery within one intelligent platform secured by Zero Trust principles.

DATA RECOVERABILITY MEASURES ARE COMMON BUT MATURITY VARIES

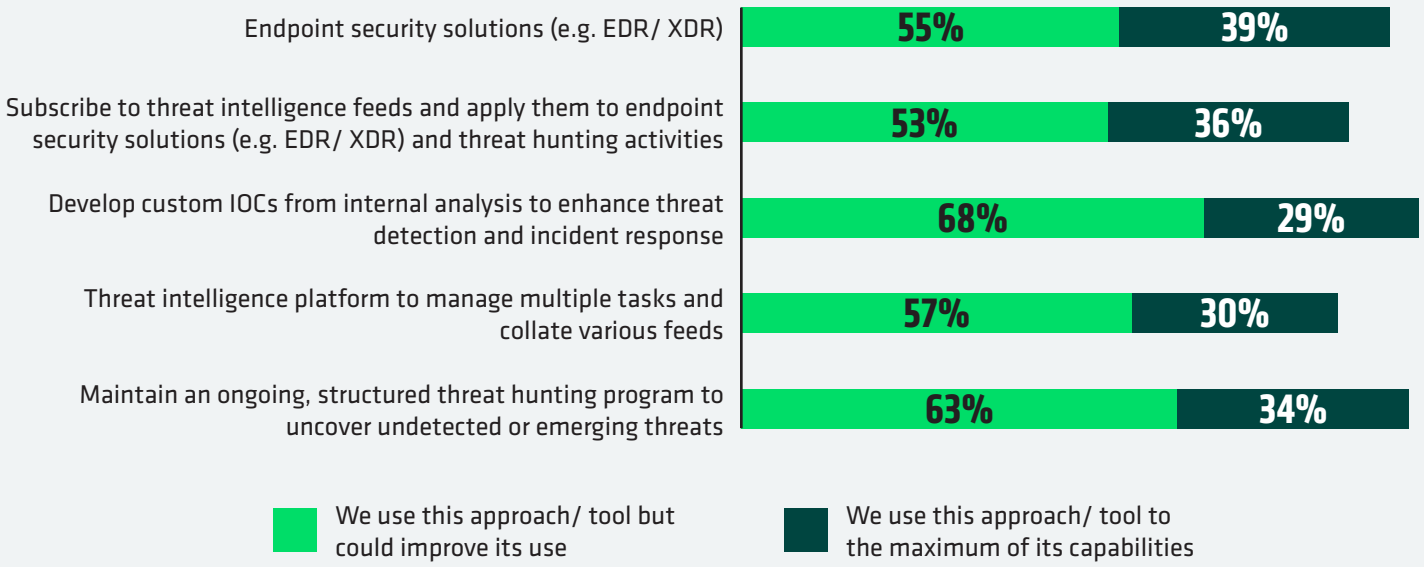
What does your organisation do to ensure that its data is always recoverable?

65%	Require additional authorisation on high-risk admin tasks associated with backup and recovery solutions
62%	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
36%	Least privilege access rights on backed up workloads

Many Indian organisations have strengthened access controls around their backup environments. Nearly two-thirds require additional admin authorisation for high-risk tasks and enforce multifactor authentication on backup solutions. About half follow the 3-2-1 backup rule or protect critical data with immutability, while only 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 UNDERUTILISED

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



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

ORGANISATIONS ARE VULNERABLE TO REINFECTION

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

66% Identify and remediate security control gaps before restoring systems to production

63% Conduct annual end-to-end simulated rehearsals including a cross functional team of technical, legal, strategic, executive and communications stakeholders

58% Use online, vaulted repository of critical systems and information to support incident response and recovery

47% Use an isolated environment for incident investigation, remediation and secure recovery

42% Immutability for all backup data

Indian organisations are advancing their approach to application resilience, but gaps remain. Most conduct simulated recovery rehearsals and address control weaknesses before restoring systems, while more than half maintain vaulted repositories of critical systems to support response and recovery. Yet fewer than half use isolated environments for secure investigation or apply immutability across all backup data. That can leave recovery processes vulnerable to reinfection or data loss. Mature cyber resilience pairs preparation with secure, verifiable recovery zones.

COMPLIANCE LEADS, BACKUP LAGS

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

Identify and resolve backup privacy and security violations for compliance

Use backup data classification to determine compliance obligations for impacted data

Identify and prioritise systems for backup

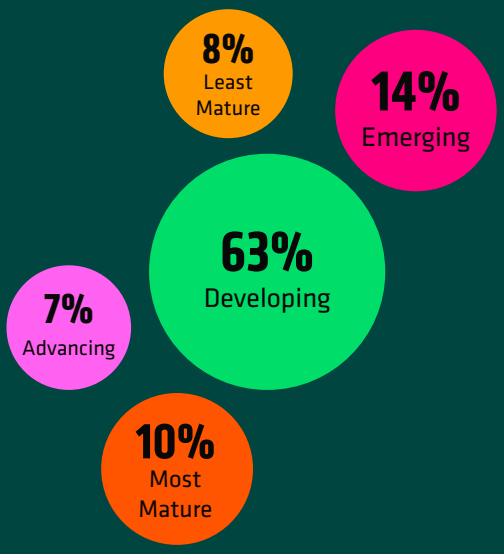
Define and understand cyberattack materiality before an incident occurs

Indian organisations are using data discovery and classification more strategically across compliance, response, and recovery. Most address privacy and security violations and apply classification to guide compliance obligations during an attack, while notably fewer assess materiality or prioritize backups based on risk. Mature cyber resilience transforms classification into a systematic capability that optimises data risk posture and strengthens 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 Indian organisations are building – or struggling to build – resilience in practice. While the majority fall into the developing stage, only 10% demonstrate the most mature, integrated capabilities that define risk-ready organisations.

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 (14%): Some resilience practices are in place, but inconsistently. Organisations 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.

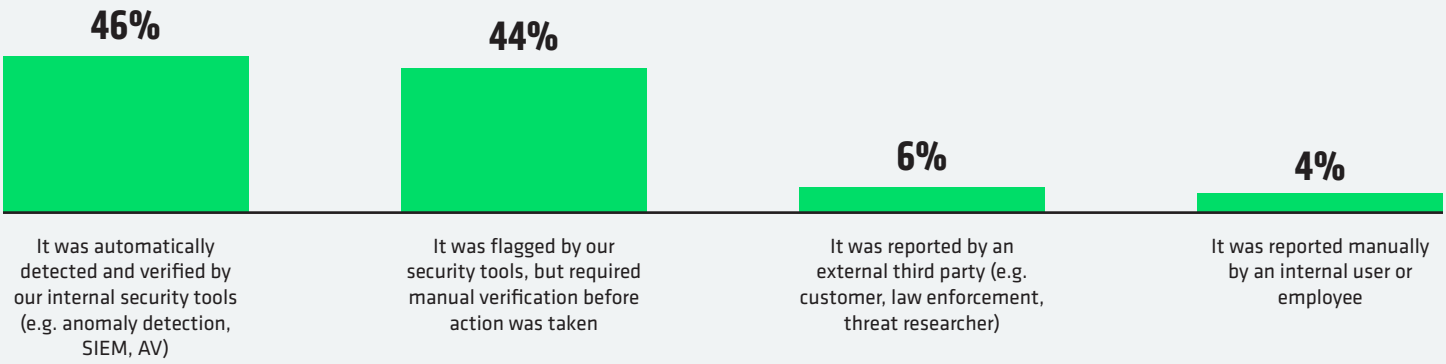
Developing (63%): Core practices such as backups, admin controls, and threat intelligence are more common, though still uneven. Recovery environments, compliance checks, and security gap remediation are applied sporadically, leaving resilience efforts partially effective.

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 optimised, and some gaps remain around isolated recovery and full compliance coverage.

Most Mature (10%): 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.

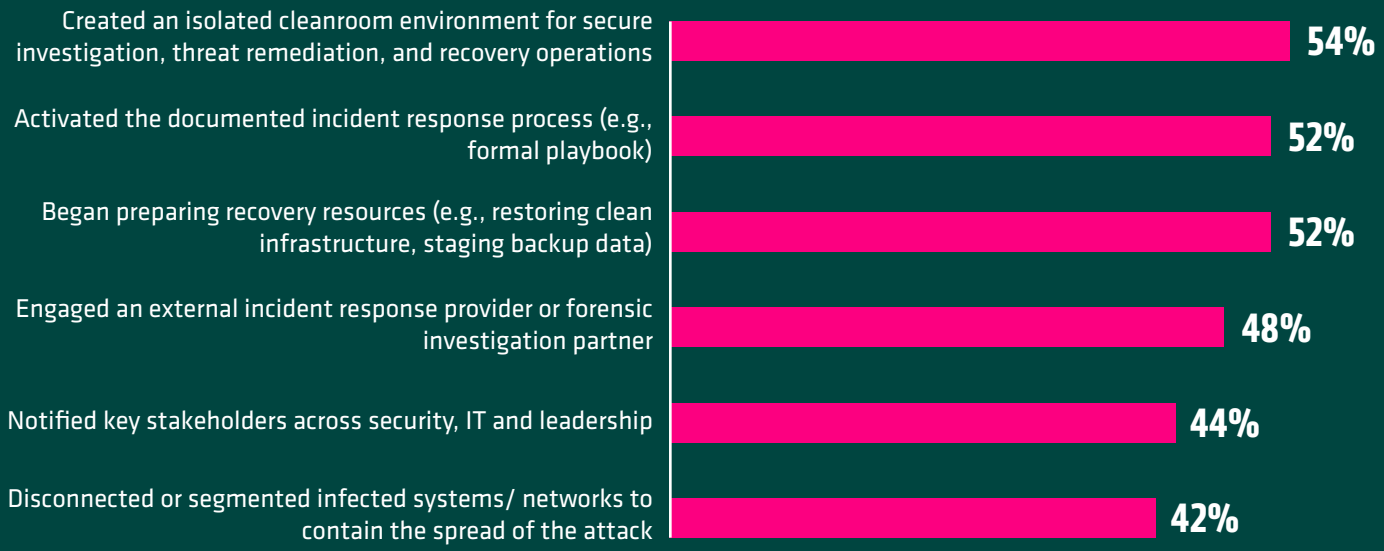
RESILIENCE UNDER FIRE

HOW TEAMS IDENTIFIED THE ATTACK



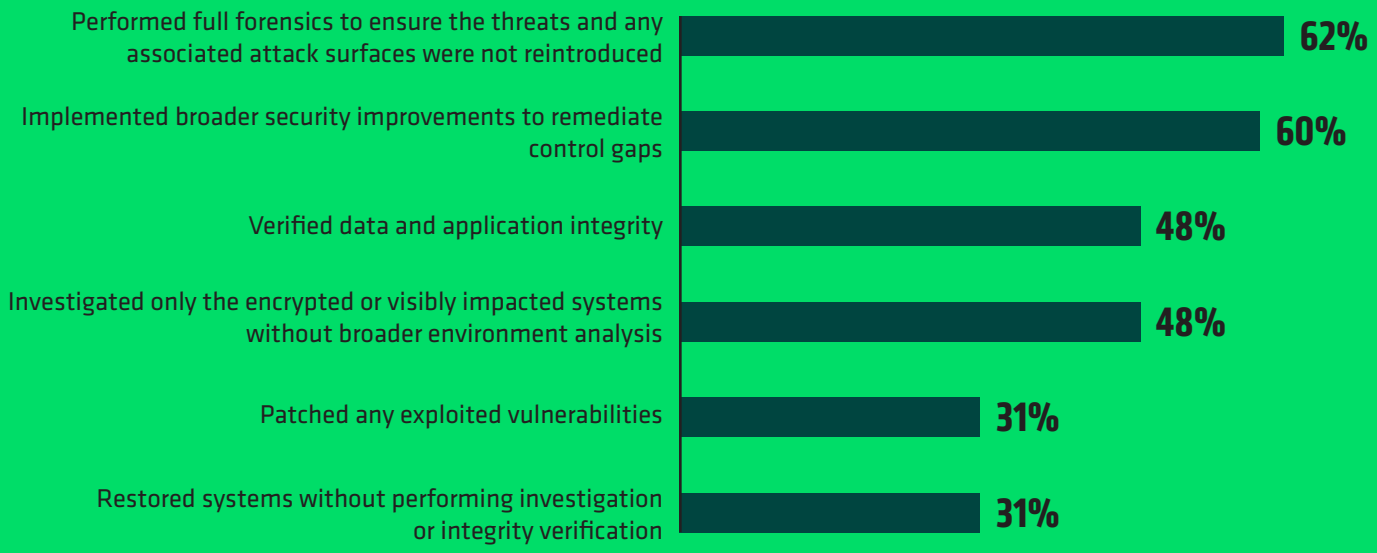
In the event of a cyberattack, most Indian organisations detect incidents internally. Nearly half said attacks were automatically identified and verified by their own security tools, while another 44% required manual verification after alerts were triggered. Only a small fraction relied on employee or third-party reports, indicating that detection is largely internal but still depends on human confirmation.

ACTIONS TEAMS TOOK AFTER CONFIRMING THE ATTACK



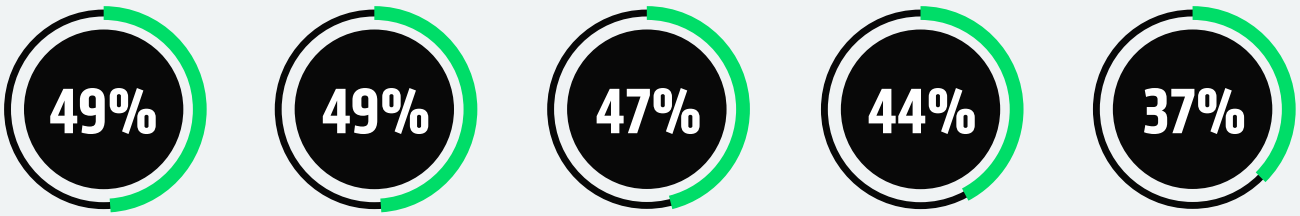
Once attacks were confirmed, more than half of Indian organisations created isolated cleanroom environments for secure investigation and remediation or began restoring clean infrastructure and staging backup data. A similar share activated their formal incident response playbook, while nearly half engaged external forensic experts. However, fewer notified key stakeholders or segmented infected systems, indicating that response actions remain uneven across critical steps.

STEPS TAKEN BEFORE BRINGING SYSTEMS AND DATA BACK ONLINE



Before bringing systems back online, most Indian organisations performed at least some level of forensic and remediation work. Nearly two-thirds conducted full forensics to ensure threats were eradicated, while six in ten strengthened controls to remediate security gaps. About half verified data integrity or limited their investigation to visibly affected systems. Yet nearly a third restored systems without full validation, leaving openings for reinfection and residual risk.

CHALLENGES TEAMS FACED DURING THE ATTACK



Teams reported significant challenges throughout the recovery process. Nearly half struggled to communicate or coordinate while critical systems remained offline. Many faced pressure from leadership to restore operations before remediation was complete. Security tool evasion, reinfection, and lack of clean recovery points further compounded difficulties.

WHERE RESILIENCE INVESTMENT STILL FALLS SHORT

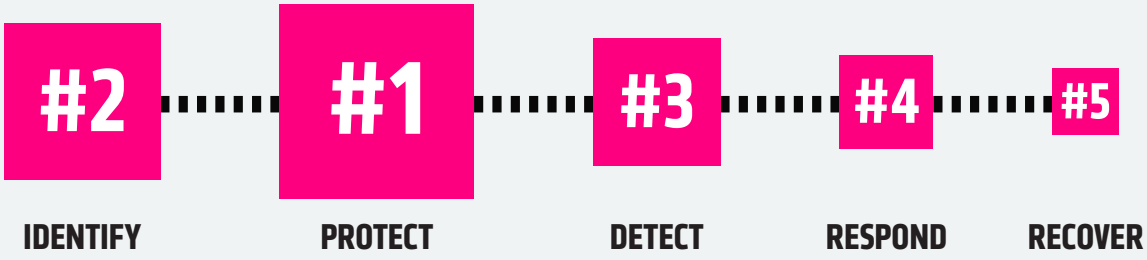
Even well-prepared organisations struggle to sustain resilience once an attack unfolds. As operational pressure mounts, coordination gaps, incomplete remediation, and reinfection risks expose how fragile recovery can be without unified processes and continuous assurance.

These weaknesses are mirrored in how Indian organisations allocate their cyber-resilience budgets today. While most align with national standards and guidance from CERT-In, the RBI, and ISO/IEC 27001, many also reference the NIST Cybersecurity Framework to benchmark maturity across its five core functions—Identify, Protect, Detect, Respond, and Recover.

When asked how they allocate budgets across these areas, most continue to concentrate investments in prevention, protection, and detection, while comparatively fewer resources are directed toward response and verified recovery. The result is a maturity curve still weighted toward defence rather than restoration, highlighting an 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 Indian organisations 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-seven percent of Indian organisations 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 defence by the end of 2026. Nearly half (48%) anticipate AI will support human decision-making, enhancing analysis and recommendations, with humans remaining in control of final actions. Almost as many (46%) 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 Indian organisations 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 organisations 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 organisations in the US (500), Brazil (200), UK (400), Germany (400), France (400), UAE (100), Australia (200), South Korea (200), Japan (400), India (200), and Singapore (200). The organisations 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

2000066-001 IND 11-2025