COHESITY

SEPTEMBER 2026

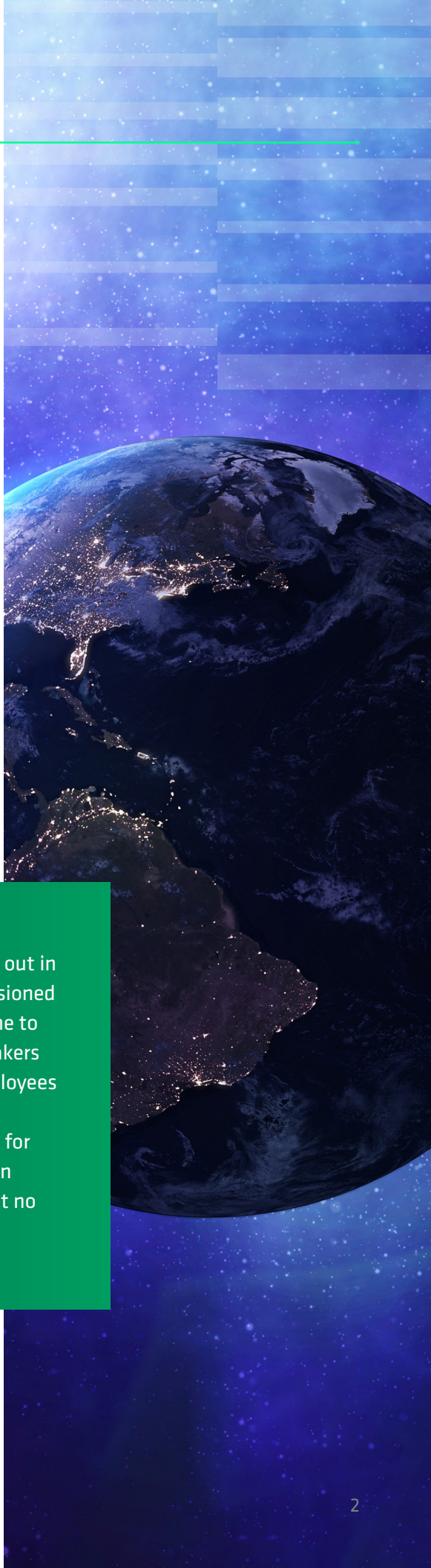
GLOBAL CYBER RESILIENCE REPORT

Cyber recovery plans weren't designed for this moment

The problem isn't the playbook. It's the world it was written for.

Most cyber recovery playbooks were built around a set of assumptions that made sense when they were written. They assumed the scope of an incident would be understood, dependencies would be mapped, and recovery would follow a predictable sequence.

Today's threat environment challenges those assumptions. AI and autonomous agents are creating new paths to compromise and accelerating how quickly vulnerabilities are discovered and weaponized. Cloud and SaaS expansion continues to increase the number of systems, services, and dependencies involved in recovery. As incidents unfold, scope expands; unexpected dependencies appear, and the sequence envisioned in the plan no longer matches the reality on the ground.



3,200
IT and security decision-makers

1,000+
employees per organization

12
countries

To better understand how recovery plays out in today's environments, Cohesity commissioned independent research firm Vanson Bourne to survey 3,200 IT and security decision-makers at organizations with 1,000 or more employees across 12 countries. The resulting report, "Cyber Recovery Plans Weren't Designed for This Moment," suggests many still rely on recovery approaches built for a world that no longer exists.

KEY FINDINGS

Most recovery plans are built on assumptions that may not survive a real attack.

Ninety-three percent of survey participants say their cyber response and recovery plans rely on all five common assumptions tested in this study, to some degree. Reliance is highest among those expressing complete confidence in their cyber resilience strategy.

Many organizations focus their recovery plans on the wrong finish line.

Over three-quarters (78%) agree that their plans focus more on restoring systems than on maintaining critical operations and serving customers during recovery. Many (72%) also prioritize speed of recovery, even over certainty that restored systems are clean and safe.

Few have proven what their business needs to keep operating through recovery.

Only 22% have formally documented and tested a Minimum Viable Company (MVC), the smallest, essential version of the organization that can continue operating while broader recovery efforts continue. Among that group, 92% say their MVC informed or influenced their recovery priorities.

AI is becoming operational before it becomes recoverable.

While 99% of respondents use AI systems, applications, workflows, or machine learning models, only 39% say their cyber response and recovery plans comprehensively account for attacks targeting them.

Frontier AI will require a new generation of cyber recovery planning.

Eighty-three percent of respondents believe their existing recovery plans would require moderate to significant changes if frontier AI advances capabilities such as vulnerability discovery, exploit development, and multi-step intrusions. Only 3% view their current plans as equipped for those conditions.

This report examines where recovery efforts become more difficult than expected, the obstacles encountered during response and recovery, how enterprises are defining and testing an MVC, and how AI is reshaping both cyber threats and cyber resilience.

5 ASSUMPTIONS SABOTAGING CYBER RECOVERY

Every recovery plan is a bet. It reflects deliberate choices about what organizations believe will happen when systems fail, and pressure mounts. The challenge is that today's threat environment increasingly tests those beliefs. The percentage of IT and security operations decision-makers with complete confidence in their cyber resilience strategy fell from 47% in 2025 to 37% in 2026, while the percentage reporting that their strategy requires improvement increased from 53% to 62%.

Does your organization have a cyber resilience strategy that you believe is adequate for today's threats and challenges?

Yes, we have a strategy, and I have complete confidence in it (it needs no/minimal improvement)

Yes, we have a cyber resilience strategy, but it requires improvement

2025 figures are from Cohesity's November 2025 Global Cyber Resilience Report.

5 ASSUMPTIONS SABOTAGING CYBER RECOVERY

An overwhelming majority of survey participants say their response and recovery plans rely on all five of the assumptions assessed in this study. Reliance is strongest among those who express complete confidence in their cyber resilience strategy and consistently lower for those who believe significant improvement is needed. This implies confidence may be rooted more in faith than proven testing under today's conditions.

Organizations whose response and recovery plans rely on the following assumptions to some or a great extent

86%	85%	84%	83%	79%
Once core systems are restored, **business operations can safely resume** with trust in the recovered environment	Decision-makers will have **adequate information and clarity** when recovery actions are required	There will be **sufficient visibility into system and data dependencies** to sequence recovery accurately in advance	**Incidents can be fully contained** before recovery begins (the scope of affected systems will be known and stable)	Recovery can proceed in a mostly **linear, step-by-step sequence** without significant backtracking

93%

of cyber response and recovery plans rely to at least some degree on all five of these common assumptions

The threat landscape changed. Investment priorities haven't.

If the assumptions above are the bet, spending reflects where organizations are putting their chips. We asked respondents how cyber resilience investment is allocated across the five NIST Cybersecurity Framework functions: Identify, Protect, Detect, Respond, and Recover. Investment priorities remain largely unchanged from last year. Protect remains the top area of investment, followed by Identify and Detect, while Respond and Recover continue to receive the smallest share, accounting for just 34% of total cyber resilience spending. Notably, nearly three-quarters (73%) of organizations agree their cyber resilience investment is weighted too heavily toward prevention at the expense of response and recovery.

RECOVERY PLANNING MEETS REALITY

Our study draws a clear distinction between everyday security events and the incidents that materially disrupt how a business operates. Throughout this report, we use the term "material cyberattack" to describe deliberate attempts to compromise, disrupt, or gain unauthorized access to systems, networks, or data that result in measurable financial, operational, reputational, or customer impact. These attacks are growing in frequency.

The scope rarely stays where it started.

Seven in 10 (70%) organizations that experienced a material cyberattack in the past 12 months saw the scope of affected systems expand beyond their initial assessment during recovery. These attacks often reveal themselves over time. New systems come into scope. Additional compromise is uncovered. And recovery teams find themselves responding to a larger incident than they initially identified.

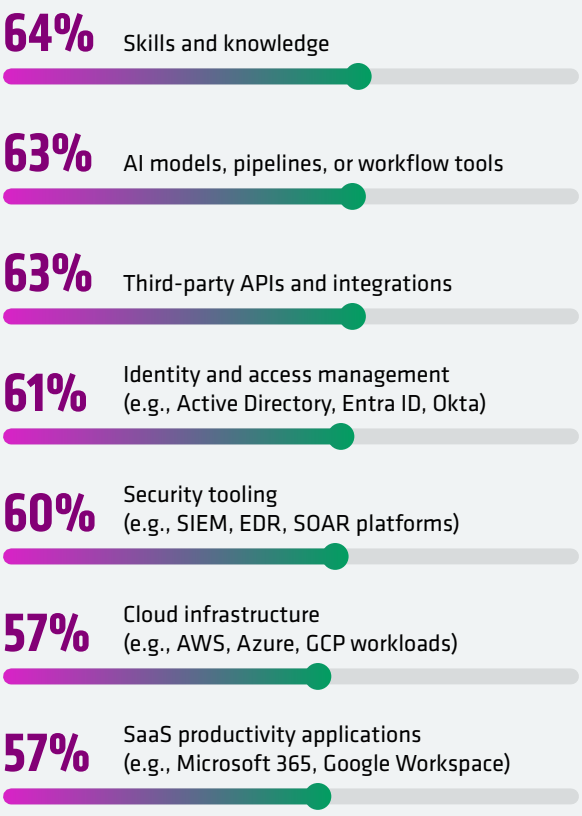
Dependency gaps emerge.

Gaps emerged across the range of dependencies identified in this study, including AI models and pipelines, third-party integrations, and identity management. Among organizations that experienced a material cyberattack in the past 12 months, 61% on average found moderate to significant gaps in how their response and recovery plans accounted for dependencies. The findings don't point to any single dependency as the primary challenge. Instead, they show how difficult it can be to account in advance for the many interconnected technologies, services, and people that modern recovery depends on.

- Almost three-quarters (73%) of surveyed organizations say they experienced a material cyberattack in the past 12 months, up from 54% in 2025.
- When these attacks occur, recovery often takes longer than expected. For three in four (76%) organizations, actual recovery exceeded their recovery time objective (RTO). On average, recovery took nearly twice as long as their RTO.
- Eighty-eight percent of respondents say their recovery plan is likely to require workarounds or improvisation during a real attack.

During the cyberattack to what extent did your organization identify gaps in how its response and recovery plan accounted for the following dependencies?

Significant or moderate gaps



Showing data for organizations that experienced a material cyberattack in the past 12 months.

RECOVERY PLANNING MEETS REALITY

Restored doesn't mean ready.

Bringing a system back online isn't the same as trusting it. Before reconnecting restored systems or data to production environments, respondents used a range of validation practices, including data integrity checks, security scans, dependency validation, and isolated testing. Yet no single method was applied consistently across the board, and independent third-party forensic review was the least common verification practice.

Before reconnecting restored systems or data to production environments, what steps did your organization take to verify they were safe to use?

52%

Conducted data integrity checks before reconnecting restored systems or data

51%

Validated that key dependencies were functioning correctly before reconnecting

50%

Ran security or threat scans on restored data or systems

49%

Tested restored systems in an isolated or clean environment

48%

Verified restore points against known-good or immutable backups

39%

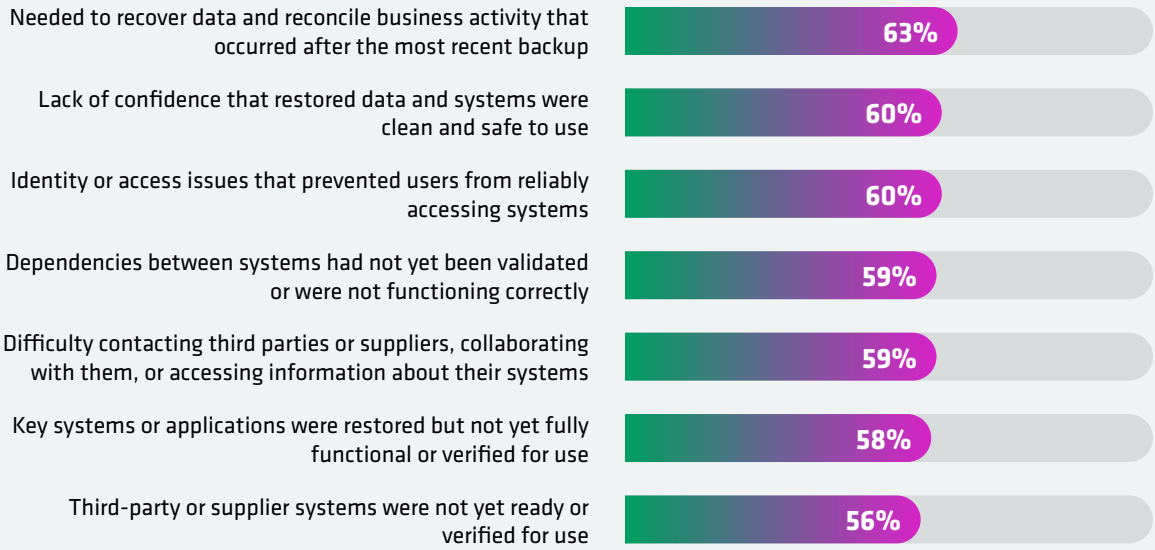
Used third-party forensic review to validate systems before reconnecting

Showing data for organizations that experienced a material cyberattack in the past 12 months.

RECOVERY PLANNING MEETS REALITY

Restoring systems may be a milestone in recovery, but for many it's not the point at which normal business operations can safely resume. For example, 68% of organizations that experienced a material cyberattack in the past 12 months admit they don't always test identity systems after the attack to verify that persistence mechanisms and attacker access have been eliminated. In many cases, delays also continue long after systems have technically been restored. More than half of the survey participants who experienced a material cyberattack in the past 12 months also reported moderate or significant delays tied to every factor measured in this study.

After systems were restored following the cyberattack, to what extent did each of the following delay your organization's ability to resume normal business operations?



Showing data for organizations that experienced a material cyberattack in the past 12 months.

Organizations that experienced a material cyberattack in the past 12 months

69%

encountered **all seven recovery delay factors**

84%

agree that differences between IT and security teams can **delay decisions about when systems are safe** to bring back online

76%

prioritize speed of recovery over certainty that restored systems are clean and safe

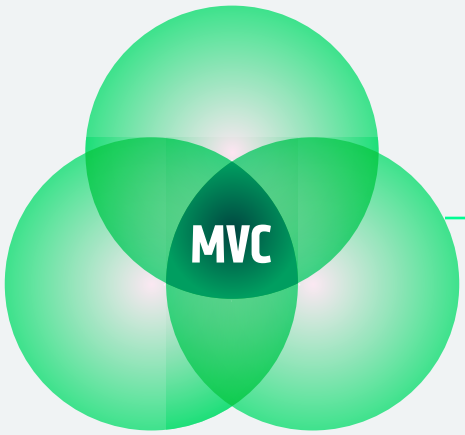
MVC'S POTENTIAL REMAINS LARGELY UNTAPPED

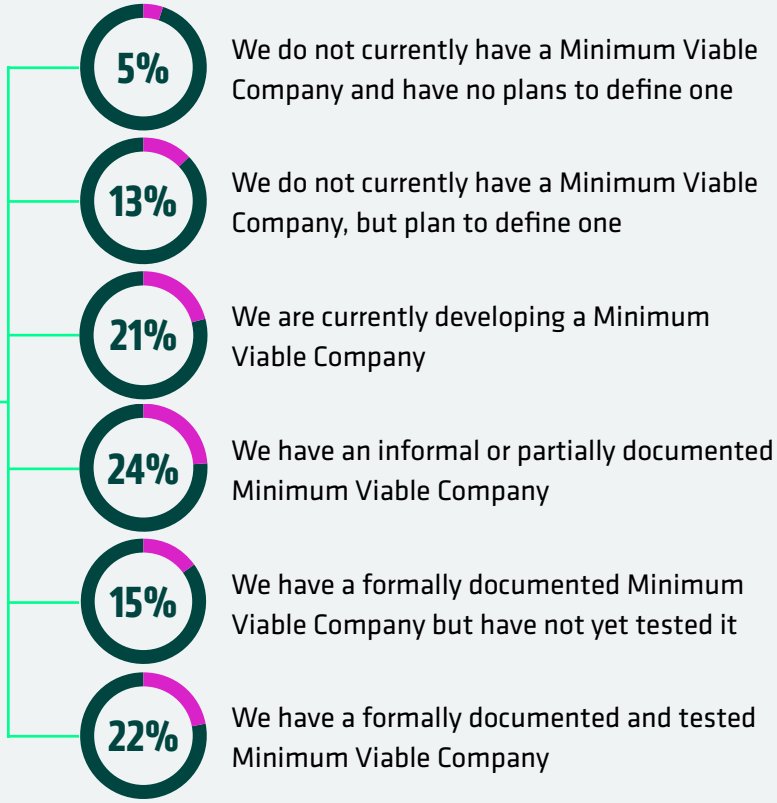
Reliance on questionable assumptions and outdated approaches to response and recovery helps explain why so many plans remain focused on restoring systems. More than three-quarters (78%) of IT and security operations decision-makers agree that their cyber response and recovery plan focuses more on restoring systems than on how the business will continue to serve customers and maintain critical operations during recovery.

A Minimum Viable Company (MVC) is the smallest, essential version of the business that can continue serving customers and maintaining critical operations while broader recovery continues. It's a defined operating model for what matters most, decided before a crisis hits.

Despite growing attention to MVC planning, relatively few organizations have formally documented and tested one. Just 22% of survey participants say they've done so. Among those with a formally documented and tested MVC, however, 92% say it informed or influenced their recovery priorities. Within that group, 64% say the MVC directly determined what was prioritized and restored first during a cyberattack.

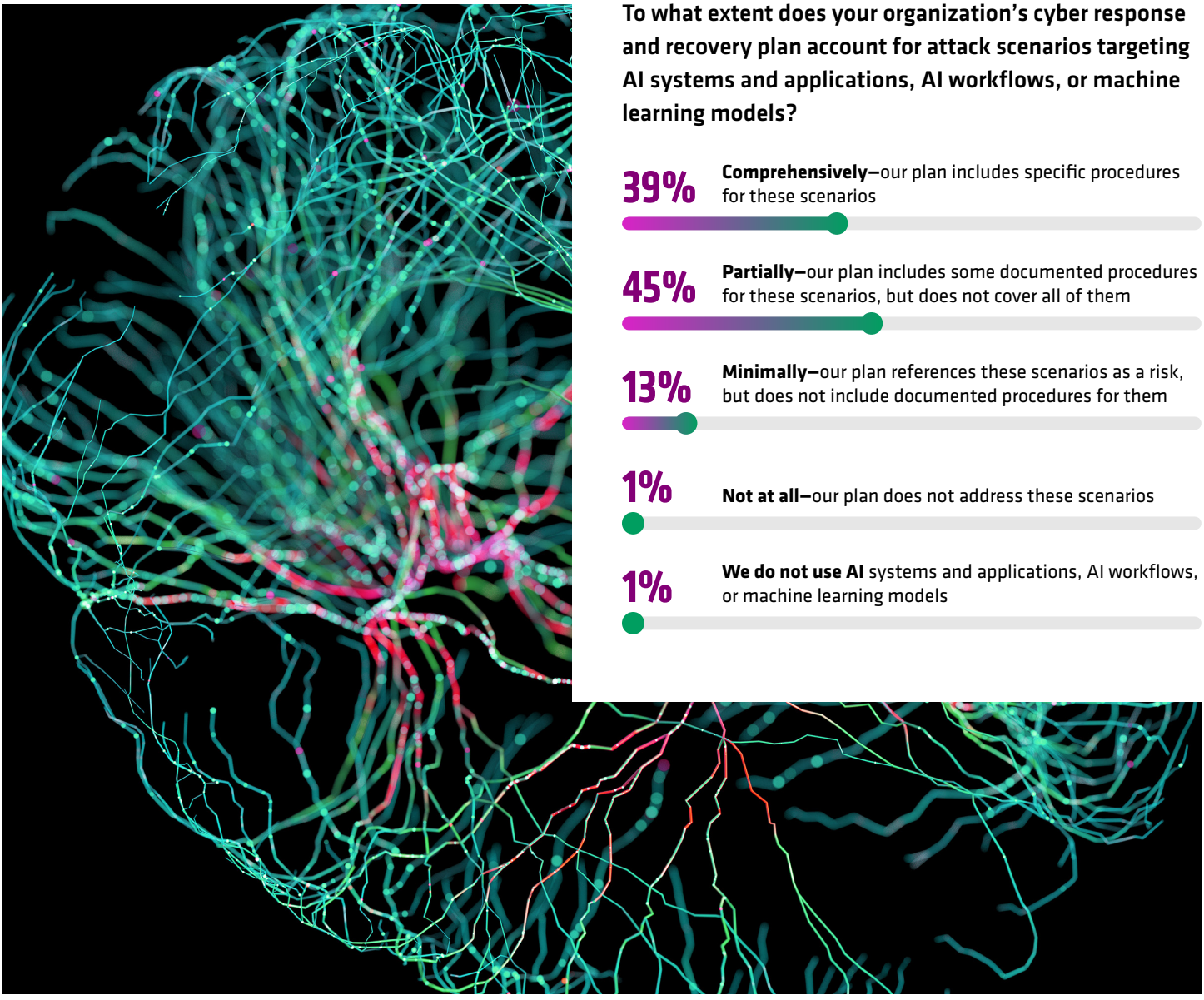
Which of the following best describes your organization's current approach to defining a Minimum Viable Company?





AI IS BECOMING OPERATIONAL BEFORE IT BECOMES RECOVERABLE

Every assumption explored in this report becomes harder to maintain when AI enters the environment. AI introduces new systems, workflows, models, and dependencies that must be understood, protected, and recovered. Yet recovery planning has not kept pace with AI adoption. While 99% of respondents report using AI systems, applications, workflows, or machine learning models, only 39% say their cyber response and recovery plan comprehensively accounts for scenarios where these might be attacked.



To what extent does your organization's cyber response and recovery plan account for attack scenarios targeting AI systems and applications, AI workflows, or machine learning models?

39% **Comprehensively**—our plan includes specific procedures for these scenarios

45% **Partially**—our plan includes some documented procedures for these scenarios, but does not cover all of them

13% **Minimally**—our plan references these scenarios as a risk, but does not include documented procedures for them

1% **Not at all**—our plan does not address these scenarios

1% **We do not use AI** systems and applications, AI workflows, or machine learning models

AI IS BECOMING OPERATIONAL BEFORE IT BECOMES RECOVERABLE

This gap extends beyond recovery planning. Organizations must also be able to verify that AI models, associated data, and AI-driven processes remain trustworthy after an incident. More than half (58%) aren't very confident in their ability to verify the integrity of AI models and related data following a cyberattack. Confidence, however, varies significantly based on the maturity of AI recovery planning. Among survey participants who comprehensively address AI-specific attack scenarios in their recovery plans, 71% are very confident in their ability to verify AI integrity, compared with just 24% of those that address these scenarios partially and 16% of those that address them minimally.

How confident, if at all, is your organization in its ability to verify the integrity of AI models and associated data following a cyber incident?

41%

Very confident

We have established procedures and tools to verify the integrity of AI models and associated data

51%

Somewhat confident

We have some capability but acknowledge gaps

7%

Not very confident

We lack adequate tools or processes to verify the integrity of AI models and data

1%

Not at all confident

We have no capability to verify AI model or data integrity following an incident

In a similar pattern, more than half (56%) say they're not well prepared to detect, contain, and recover from unintended or incorrect actions taken by AI agents, copilots, or AI workflows. For organizations whose recovery plans comprehensively account for AI-related scenarios, preparedness rises substantially (80%). Just 22% of organizations whose plans address these scenarios only partially say they're well prepared, falling to 11% among those whose plans address them minimally.

How prepared is your organization to detect and contain unintended or incorrect actions taken by AI agents, copilots, or AI workflows, and recover affected systems or data?

44%

We are well prepared, with established and tested processes to detect, contain, and recover from these scenarios

44%

We have processes to detect, contain and recover from these scenarios, but they are not fully developed or tested

11%

We have limited ability to detect, contain, or recover from these scenarios

1%

We are not prepared to manage these scenarios

AI IS BECOMING OPERATIONAL BEFORE IT BECOMES RECOVERABLE

AI changes what recovery must prove.

Although most enterprises are already incorporating AI into business operations, many believe the greater challenge lies ahead. We asked how much existing recovery plans would need to change to remain effective if frontier AI continues to advance capabilities such as vulnerability discovery, exploit development, and multi-step intrusions. This question wasn't about attacks organizations have already experienced. It was about whether recovery plans are built for what is coming next. Nearly every participant surveyed said change is required to address emerging threats from frontier AI capabilities.

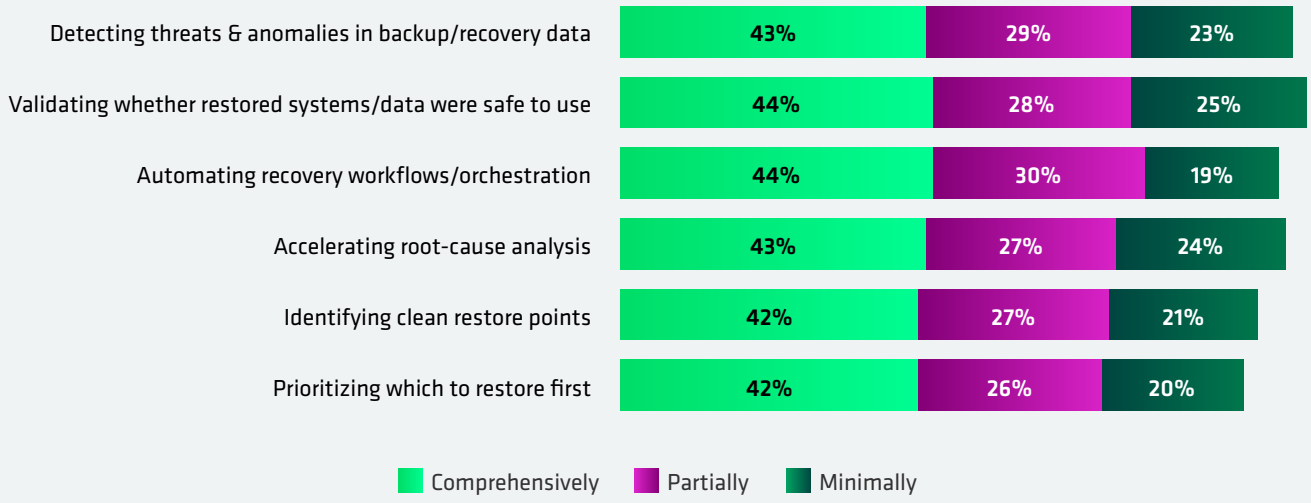
- Only 3% say their current recovery plan is equipped to withstand them
- 83% say moderate to significant change would be necessary to address frontier AI-based attacks

Where AI is already helping the defense.

Organizations that experienced a material cyberattack in the past 12 months also report using AI-enabled tools across a wide range of response and recovery processes. Four in five (80%) say those tools made a moderate to significant contribution across every area measured, on average, from threat detection and root-cause analysis to recovery orchestration and identifying clean restore points.

Additionally, organizations that comprehensively account for attack scenarios targeting AI systems, applications, workflows, or models are also consistently more likely to report significant contributions from AI-enabled tools during response and recovery. The same organizations preparing for AI as part of the attack surface are often the ones using AI most effectively during an attack.

AI-enabled tools contributed significantly to help in the following areas during the material cyberattack



Response and recovery plan accounts for attack scenarios targeting AI systems/applications/workflows or ML models.

RECOVERY FOR THIS MOMENT AND THE NEXT

If most cyber recovery plans weren't designed for a world that keeps changing, the next generation of recovery planning must be. In an environment where vulnerabilities are weaponized faster, attack paths multiply, and AI is reshaping both the threat landscape and business operations, resilience depends on continuously testing assumptions before a crisis puts them to the test.

The next generation of response and recovery planning starts with a few fundamental shifts:

- Don't just document your recovery plan. Test it under realistic conditions.
- Move beyond system recovery. Think about the business impact. Define and test a Minimum Viable Company.
- Treat identity and other mapped critical dependencies as recovery foundations.
- Ensure recovered systems and data can be trusted, not just restored.
- Extend trusted recovery practices to AI models, agents, and workflows.

Discover tools and guidance to help turn planning into operational readiness:

- Download the Cohesity 5 Steps of Cyber Resilience© eBook
- Book a Ransomware Resilience Workshop
- Explore Cohesity's cyber resilience solutions

METHODOLOGY

Cohesity commissioned independent research firm Vanson Bourne to conduct this study, which surveyed 3,200 IT and security decision-makers at organizations with 1,000 or more employees. The survey was administered in July 2026 across Australia, Brazil, France, Germany, India, Japan, Saudi Arabia, Singapore, South Korea, the United Arab Emirates, the United Kingdom, and the United States. Year-over-year comparisons throughout the report reference findings from Cohesity's November 2025 Global Cyber Resilience Report.

COHESITY

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