veeam Insights

Data Trust and Resilience Report 2026

Executive Summary

Organizations today face a paradox. Digital transformation, cloud adoption, and AI have increased the value of enterprise data, but they have also expanded the attack surface around it. Data now moves across clouds, applications, AI models, agents, and automated systems faster than most organizations can track.

Despite that complexity, most organizations believe they're prepared.

The bottom line: In our survey of more than 900 security leaders across the C-suite and frontline security roles, **90%** said they were very to extremely confident they can recover from a cyber incident within their defined recovery time objectives (RTOs).

Actual outcomes are less reassuring. Among organizations that experienced a cyber incident in the past 12 months, **more than 40%** reported customer or constituent disruption or financial loss.

Ransomware outcomes are even tougher. For incidents that contributed to operational loss or encryption of data, only **28%** fully recovered all affected data. Another **29%** ended up with data loss, downtime, or business disruption.

These measures are not identical to RTO performance, but together they tell a consistent story: Confidence in recovery is not the same as demonstrated recovery capability. In interviews, many organizations equate resilience with having backups, policies, or insurance in place. Real resilience requires more. It demands clear visibility into where data lives and how it's used, enforced controls that reduce exposure in practice, and recovery that's proven through testing, not assumed.

As organizations integrate AI into business operations, the stakes rise further. AI introduces new data flows, new attack surfaces, and new governance challenges. In the emerging agentic era, AI systems increasingly act on users' behalf, moving data and triggering actions with less direct human oversight. In many cases, AI adoption is moving faster than organizations' ability to secure and govern the underlying data, widening the mismatch between perceived readiness and operational reality.

Recovery Confidence vs. Operational Alignment

90%

reported being very to extremely confident in meeting RTOs.

69%

say their RTOs are fully aligned with business continuity goals.

Organizations with stronger recovery outcomes share four defining capabilities:

1. **Clear visibility** into data and AI risk across the enterprise.
2. **Enforced security controls**, not policy alone.
3. **Proven recovery capabilities** that are tested and validated.
4. **Executive alignment** around risk ownership and reporting.

Together, these capabilities form the foundation of modern cyber resilience. Organizations that build them are better positioned to withstand cyber incidents and to safely unlock the value of AI and digital innovation.

The Confidence Gap

Nearly 3 in 10 organizations have experienced a cyber incident in the past 12 months that resulted in data loss, downtime, or business disruption.

The pattern is similar among organizations hit by ransomware. Of those that experienced a ransomware attack in the past 12 months, **56%** said attackers succeeded in encrypting or exfiltrating data. Among ransomware-affected organizations, only **28%** fully recovered their data, while **44%** recovered less than 75% of their affected data.

Taken together, these results reinforce the central theme of this report: Confidence is common, but validated recovery capability is not. When organizations don't routinely test recovery under real-world conditions, they can overestimate readiness until an incident makes the gaps visible.

Interviews suggest that confidence in recovery is often shaped by the presence of testing and planning, even when the frequency and realism of those tests are constrained by operational and business pressures.

Organizations are also confronting a second force that can widen the same gap. As AI becomes more embedded in everyday workflows, it introduces new data paths, new tools, and new governance requirements. Without clear ownership and updated security policies, AI can expand risk faster than teams can manage it.

When incidents do occur, downstream impacts are often significant. Among organizations that experienced a cyber incident:

42%

reported customer or constituent service disruption.

41%

reported financial loss or revenue impact.

38%

experienced extended downtime of critical systems.

AI Adoption Outpaces Risk Visibility

AI is moving from experimentation to everyday execution. Security leaders report that AI is already embedded in core processes, and many expect its role to expand quickly. That momentum is creating a new reality where AI risk is no longer isolated to model security. This is a data governance and operational resilience problem.

The challenge is visibility. AI systems introduce new data paths across users, applications, APIs, and third-party services. They can also amplify common issues like data sprawl, inconsistent access controls, and unclear ownership. When teams can't see how data is being used, shared, or retained, it becomes harder to enforce policy, detect misuse, and recover cleanly after an incident.

Just as important, AI adoption often outpaces governance. Many organizations are still deciding who owns AI risk, which teams define acceptable use, and how policy becomes enforceable controls. Without that clarity, organizations can end up with fragmented oversight, inconsistent guardrails, and slow decision-making during an incident.

This is where the recovery readiness gap shows up again. AI expands the scope of what must be protected and recovered (e.g., data, pipelines, identities, and the systems AI depends on). If AI-related data sources are not classified, controlled, and backed up with the same discipline as other critical systems, recovery plans can break down under pressure.

That visibility gap shows up clearly in the survey data:

43%

of respondents say AI tool adoption is outpacing their ability to secure data and models.

42%

say they have limited visibility into all the AI tools or models used across the organization.

40%

say security policies haven't yet been updated to include AI-specific risks, such as the use of generative AI.

25%

say shadow IT and unauthorized AI tool usage are a primary concern related to employee AI tool use and data security.

Policy Alone Doesn't Reduce Risk

To lower rising AI and data risks, organizations need AI governance approaches that extend beyond policy statements to policies that are backed by enforceable controls. One indicator of that shift is adoption of enforcement tooling such as data loss prevention (DLP). In this research, 48% of respondents said DLP controls were already in place.

Organizations with DLP in place report measurably stronger visibility and control as AI usage expands. Compared to organizations without DLP, they are:

Limited visibility into AI tools and models

39% With DLP vs **45%** Without DLP

AI adoption outpacing security controls

38% With DLP vs **48%** Without DLP

Enforceable controls help translate governance into day-to-day execution by reducing risky data movement and limiting exposure as AI usage expands.

In practice, organizations describe governance as effective only when policies are backed by controls and validation, rather than relying on intent or guidance alone.

Who Owns AI Governance?

As organizations adopt artificial intelligence across business operations, the question of **who owns AI and data risk** is becoming increasingly important.

The research shows that responsibility for AI governance is rarely shared across leadership teams. Instead, it is typically assigned to a single executive. Among organizations that experienced a cybersecurity incident:

38%

said AI and data risk governance was owned by the CISO.

17%

reported a cross-functional governance structure.

27%

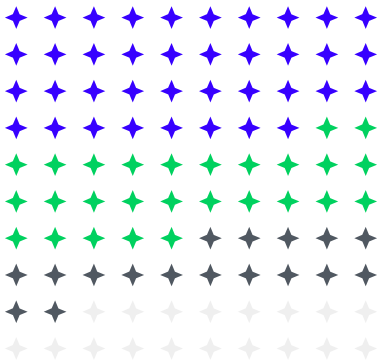
said it was owned by the CIO.

Clear ownership matters but concentrating responsibility in a single role can create blind spots. AI risk sits at the intersection of multiple domains, including cybersecurity, data governance, infrastructure, compliance, and business operations. No single executive typically has full visibility across all of these areas.

Across organizations, AI and data risk are described as spanning security, IT, data, and business functions, making shared oversight more effective than single owner models.

Organizations that adopt a cross-functional governance model by bringing together IT, security, data leaders, and business stakeholders report stronger alignment between policy, security controls, and operational recovery capabilities.

How AI and Data Risk Governance is Structured



38%
CISO accountability

27%
CIO accountability

17%
cross-functional committee

Accountability for AI and data risk governance most often rests with a single executive rather than a cross-functional group.

How Executive Alignment Impacts Recovery Success

When risk management, security operations, data governance, and IT infrastructure leaders align around shared metrics and recovery objectives, resilience becomes a coordinated capability, not a fragmented responsibility.

That matters because recovery is never owned by one team. It's a cross-functional effort that depends on shared priorities, clear ownership, and consistent reporting.

In our survey, executive leaders described different recovery experiences following ransomware and other cyber incidents. That gap reinforces a practical point: Cyber resilience depends on more than strong technology. It also depends on whether leaders agree on what "recovered" means, which metrics define readiness, and who has decision rights when the business is under pressure.

Four Practices Linked to Stronger Recovery

No single governance policy, executive hire, or technology solution guarantees recovery readiness. However, despite differences in industry, size, and maturity, the survey data points to four practices that consistently correlate with stronger recovery outcomes and are reinforced by anonymized interview insights.

1) Expanded Ownership Beyond Security Teams

> "We are constantly working toward educating each employee and having a safe zero trust approach to physical security, as well as software and hardware security, with multi-factor authentication (MFA) and biometrics. We always need to be using the latest patches, processes, and methods to make our risk surface as small as possible and are trying to use AI tools to manage known and unknown threats."
>
> **Hospitality/FinTech Conglomerate**

Organizations with stronger recovery outcomes are more likely to extend ownership of cyber resilience beyond the security function and into IT, data, and business leadership. Among respondents who did **not** experience a cybersecurity incident, **37%** reported using cross-functional policy approval committees, compared with **31%** of those that **did** experience an incident.

2) Operationalize AI Governance With Controls and Validation

> "A little over a year ago, there was an event related to one of our cybersecurity platforms that created a quality assurance issue. That forced us into a resiliency and recoverability mindset. While I think our policies were good and helped control some of the chaos, most of the recoverability was based on heroics, not necessarily from sound governance and good practices that validate that resiliency."
>
> **Fortune 1,000 Company**

Organizations reporting stronger recovery outcomes treat AI security and governance as an execution discipline, not a general priority. That includes formal AI risk management and data governance policies paired with practical controls and processes such as model validation, testing, and drift monitoring.

The survey suggests that investment aligns with more structured AI governance. Organizations that increased their data resilience budget were more likely to report having a formal AI risk management or data governance policy in place (roughly **two-thirds**) compared with those that did not increase budget (**27%**). They were also more likely to report model validation, testing, and drift monitoring (**43% vs. 26%**). These results reflect differences in governance maturity and operational practice, not a guarantee of better protection. However, they highlight the concrete steps organizations should take to better manage AI risk.

3) Communicate Cyber Risk to Business Leaders Frequently

More mature organizations tend to communicate cyber risk more frequently. In this research they also report **lower incident impact and stronger recovery outcomes**, even if the differences are modest.

Among respondents who did not experience a cybersecurity incident, **56%** reported cyber risk to the board monthly or more frequently, compared with **50%** of respondents who experienced an incident. Similarly, **40%** of respondents without an incident reported more frequent or more advanced reporting (including cyber risk quantification), compared to **35%** of those who experienced an incident.

> "At a recent tabletop exercise, the board was there at the tail end, and they had a lot of questions. One stood out: 'Wait, we don't have the ability to recover?' At the time, we didn't. We had some archaic backup capabilities. That is why we just recently invested in a very immutable infrastructure that we could recover from."

Fortune 1,000 Company

4) Track KPIs That Matter Most to Insurers and Business Leaders

Cyber insurers and business leaders increasingly ask for evidence of recovery readiness that often goes beyond attestations, using measurable KPIs tied to response and recovery performance. Tracking varies widely, and many organizations still don't measure these consistently.

In this research, respondents most often reported tracking:

Restore and recovery testing (57%).

Time to isolate and contain (42%).

Mean time to recover (56%).

Fully automated or orchestrated recovery processes (23%).

> "We communicate our cybersecurity KPIs to the board of directors in every board meeting, and they are communicated to executives weekly, monthly, and quarterly. It's part of running our operations. We need to be very clear and concise about what represents a significant risk, though, because we don't want to steal time or energy from the board of directors and the executives to do their primary jobs."
>
> **Hospitality/FinTech Conglomerate**

Investment in Cybersecurity is Increasing but not Universally

In our survey, 49% of organizations increased cybersecurity budgets year over year, while 51% stayed flat or decreased. That split helps explain why resilience outcomes vary, especially when organizations can't consistently measure readiness or validate recovery.

Tracking the Metrics That Strengthen Budgets and Recovery

Organizations with budget increases are more likely to track recovery readiness KPIs that make gaps visible and support better prioritization, including:

KPIs Used to Measure Recovery Readiness from Cyber Incidents	Budget increased	Budget not increased
Recovery time objectives (RTOs)	78%	56%
Time to isolate or contain incidents	47%	36%
Percent of recovery processes fully automated / orchestrated	32%	14%

Tracking these metrics transforms confidence into something leaders can validate when it comes to resilience.

Frequent Reporting on Risks

Budget growth is more common in organizations that report cyber risk monthly:

Reporting to the board

Frequency	Budget increased	Budget not increased
Weekly/Continuous	25%	13%
Monthly	62%	47%
Quarterly or Less	37%	52%

Reporting to the c-suite

Frequency	Budget increased	Budget not increased
Weekly/Continuous	25%	13%
Monthly	62%	47%
Quarterly or Less	37%	52%

The point is not reporting volume; it's creating a steady, decision-ready loop that keeps risk visible, priorities clear, and progress measurable.

Where Investment Turns Into Capability

Organizations with budget growth are more likely to prioritize foundational resilience capabilities.

Top Priorities for Improving Data Resilience

	Budget increased	Budget not increased
Immutable storage	38%	11%
Automated backup	42%	33%
Integrated cyber resilience and business continuity planning	16%	9%

These investments reduce uncertainty during recovery and support data trust in practice.

Cyber Investment and Recovery Performance

Budget increases correlate with stronger ransomware recovery outcomes:

Lower ransom payments

Only 33% of organizations with increased budgets paid a ransom, compared with 52% of those without increases.

Higher recovery success

40% fully recovered affected data, versus 16% among organizations without budget growth.

This is correlation, not causation. However, it aligns with a consistent pattern: Measuring readiness and investing in proven capabilities improves recovery outcomes.

Ransomware Response and Recovery by Budget Status

Outcome	Budget increased	Budget not increased
Paid ransom	32%	52%
Didn't pay ransom	52%	33%
Recovered 100% of data	40%	16%
Recovered <75% of data	29%	49%

Compliance as a Resilience Driver

Cyberattacks remain the emerging risk most likely to impact data resilience over the next 12 months (36%), but regulatory and compliance mandates are close behind (33%). Requirements also influence data placement decisions, with 58% citing data residency and sovereignty as the most important factor.

As obligations expand, compliance increasingly overlaps with resilience. Organizations need to demonstrate controls, produce evidence, and report accurately, especially after an incident.

Measured Resilience, Trusted Data

The *Data Trust and Resilience Report 2026* survey results reinforce a consistent theme: Organizations that overestimate resilience are often more exposed to data risk. Real resilience is demonstrated through validated recovery performance and supported by strong data governance, cross-functional ownership, and disciplined execution.

As AI accelerates change across data, identities, and workflows, the ability to validate recovery becomes even more critical.

Organizations that report cyber risk to leadership at least monthly are more likely to see budget growth. Organizations with budget growth are more likely to report stronger ransomware outcomes, including higher rates of full data recovery. In practice, measurement and transparency help leaders connect risk to business impact and prioritize investments that build durable data trust and resilience.

AI is moving fast, and agentic systems are accelerating how data moves, learns, and triggers actions across the enterprise. Risk rises at the same pace, which makes trusted, recoverable data essential for keeping these systems safe and reliable. Veeam helps organizations protect the data that powers their AI, contain threats quickly, and recover cleanly when disruption hits. Visit veeam.com to accelerate safe AI at scale.

→ **Check out these ten steps:**

https://go.veeam.com/10-steps-to-cloud-resilience

→ **Demystify regulatory compliance: Here are standards, frameworks and recommendations to know:**

https://go.veeam.com/demystifying-regulatory-compliance

→ **Real stories from inside the breach: This is the Wake Up podcast:**

https://go.veeam.com/wake-up-podcast.html

About Veeam Software

Veeam is the Data and AI Trust Company, specializing in helping organizations ensure their data and AI are fully understood, secured, and resilient to enable the acceleration of safe AI at scale. As the market leader in both data resilience and data security posture management, Veeam is built for the convergence of identity, data, security, and AI risk.

Veeam delivers deep contextual intelligence across every data asset, identity, and AI model. The company governs access for both humans and AI agents, automates privacy, compliance, and remediation processes, and protects and recovers organizations from modern threats – including ransomware, disasters, AI errors, and ensuring the restoration of clean, trusted data. Veeam empowers organizations to move beyond simply protecting data, enabling them to activate and unlock its full potential.

Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 82% of the Fortune 500, who trust Veeam to keep their businesses running.

Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.