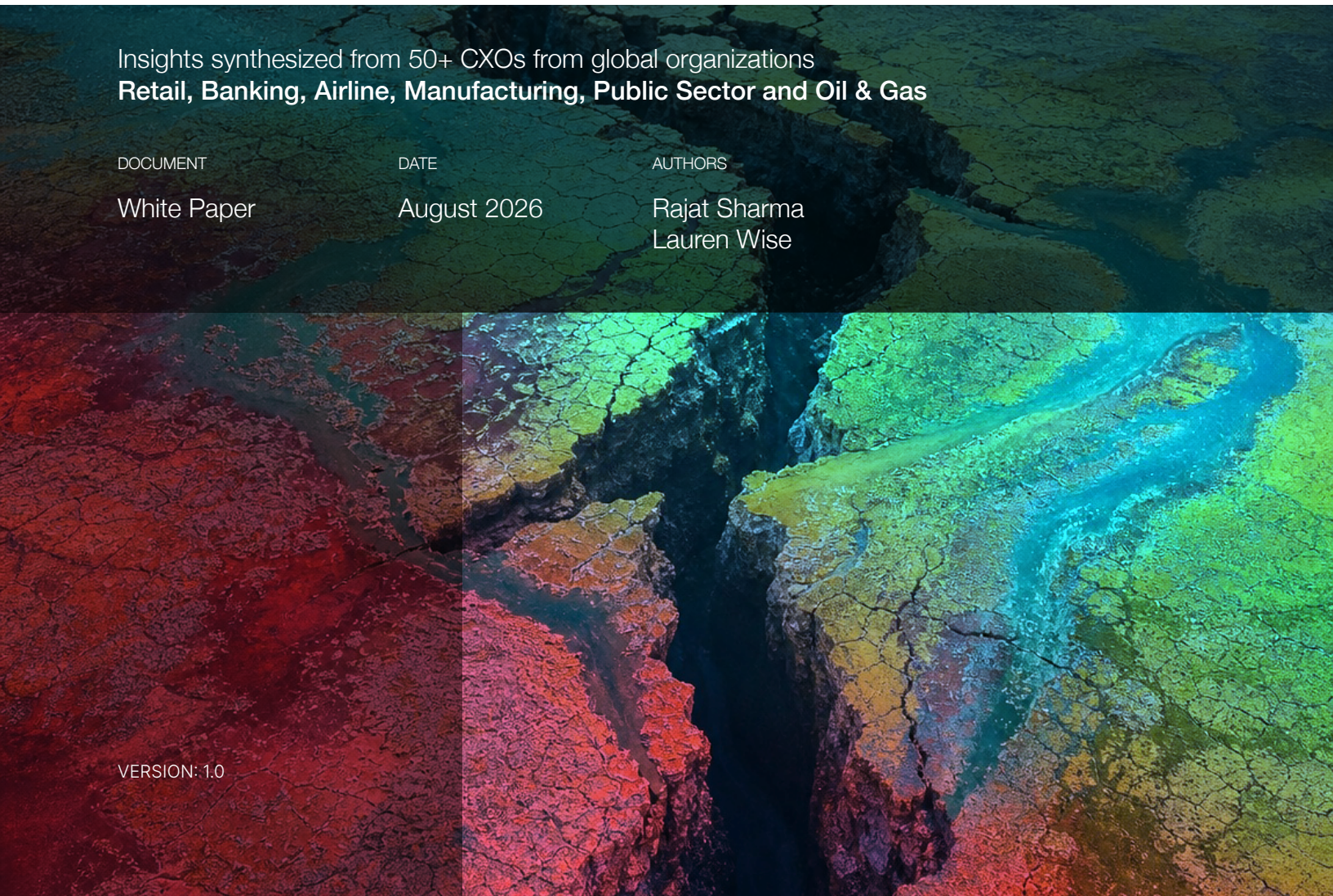
rubrik

The Cyber & AI Resilience Gap:

Observations & Opportunities for Organizations to Build Resilience That Holds Under Pressure



Insights synthesized from 50+ CXOs from global organizations
Retail, Banking, Airline, Manufacturing, Public Sector and Oil & Gas

DOCUMENT
White Paper

DATE
August 2026

AUTHORS
Rajat Sharma
Lauren Wise

VERSION: 1.0

Contents

SECTION PAGE

Executive Summary 03

Observation 1: Backup & Recovery Tool Proliferation . . 05

Observation 2: The RTO/RPO Reality Gap – Recovery Objectives Require Empirical Validation 07

Observation 3: Tier 0 and Tier 1 Infrastructure Recovery – A Significant Opportunity for Advancement 09

Observation 4: Cyber Resilience Ownership Is Assumed, Not Assigned 11

Observation 5: AI has Outpaced Governance, and the Exposure is Largely Unquantified 13

Conclusion 15

RETURN TO TOC

Executive Summary

The organizations that recover fastest from cyberattacks or major outages aren't just better prepared on paper—they've turned their plans into practiced, measurable outcomes.

Most organizations haven't reached this step. Recovery timelines are assumed, but never tested. Responsibility for resilience is unclear. And companies are running too many overlapping backup tools when far fewer would do the job better.

Rubrik's Value Economics team spoke with over 50 C-level leaders across the Retail, Banking, Airlines, Manufacturing, Oil & Gas, Technology, and Public sectors globally. The observation was consistent across all of them: most organizations believe they are more resilient than they actually are.

Closing that gap by simplifying tools, testing recovery plans, clarifying ownership, and building resilience into how the business is designed and operates is the defining challenge for security and IT leaders right now.

We have captured five key observations that explain where the gaps are, their cost implications, and what leading organizations are doing differently.

OBSERVATIONS	POTENTIAL / LEVEL OF MATURITY	IMPLICATION
Opportunities exist to consolidate backup and recovery tools	**Up to 5:1 Consolidation Potential**	Organizations are leveraging Two and sometimes up to five separate backup and recovery tools today, when one single platform is possible. Numerous tools bring increased cost, complexity, and added risks to cyber resilience and organizational recovery.
Recovery time and recovery point objectives (RTO/RPO) are not empirically tested	**Limited Empirical Testing**	Fewer than 10% of organizations regularly perform RTO/RPO testing under simulated, realistic crisis conditions that incorporate communications and executive decision-making, regulatory reporting, and business recovery.
Business critical infrastructure recovery is a challenge	**Undefined or Developing Maturity**	Organizations are experiencing cyber recovery durations spanning weeks or months, far exceeding committed recovery timelines of hours or days for business-critical infrastructure.

CONTINUED ON NEXT PAGE

EXECUTIVE SUMMARY

RETURN TO TOC

OBSERVATIONS	POTENTIAL / LEVEL OF MATURITY	IMPLICATION
Cyber resilience lacks an accountable leader	**No End-To-End Owner**	Without a dedicated cyber resilience leader, organizations may lack unified ownership and strategic coordination during a major business-impacting event, resulting in fragmented preparedness, slower recovery, and greater potential for business disruption.
AI has outpaced Governance	**Unquantified financial exposure**	More than 80% of organizations engaged are actively seeking advisory support on AI governance and deployment, creating new categories of critical data that aren't yet protected and generating possible future delays as AI deployments continue to scale.

The Core Observation

Organizations at the forefront of cyber and AI resilience share three attributes: a unified technology architecture for backup and recovery that eliminates coverage gaps, empirically validated recovery timelines for critical systems, and clear executive ownership of cyber and AI resilience. Each of these attributes is achievable, but may require a shift of focus and transformation.

RETURN TO TOC

Observation 1: Backup & Recovery Tool Proliferation

One of the most consistent observations from our conversations was the degree to which enterprise data protection architectures have evolved organically over time. On average, organizations were operating two to five or more separate backup tools simultaneously—a figure that reflects years of M&A activity, departmental purchasing decisions, and point-solution adoption without a unifying architectural vision. For some organizations, the number is considerably higher.

What the Data Shows

This pattern appears across multiple sectors. For example, within the airline industry, we identified five or more parallel solutions operating within a single organization spanning cloud, databases, Kubernetes, and identity backup.

According to Rubrik Zero Labs research, 90% of IT and Security leaders surveyed agreed that identity driven cyber attacks are the top threat to their organizations. Additionally, of another group who had experienced a cyber attack within the previous year, 35% said the threat actors were completely successful in harming their backup and recovery solutions.

While cloud and on-premise backups tend to be the primary priority, backup and recovery coverage for Microsoft 365 and identity infrastructure is often overlooked. Fewer than 20% of those we spoke with claimed full resilience and recovery capabilities.

The consequence of fragmented toolsets and missing coverage extends beyond licensing costs. When downtime or a cyber incident occurs, teams navigating multiple management consoles, disparate recovery workflows, and siloed datasets face compounded complexity, increased investigation, and recovery time across multiple teams–at the precise moment when speed and clarity are most valuable.

The Opportunity Forward

Backup and recovery tool consolidation represents an opportunity for both cost reduction and resilience enhancement. The most effective leaders frame it as both. For consolidating organizations, a unified approach expands coverage to the majority of “crown jewel” and critical systems, enabling significant, near-zero RTOs.



Organizations that have completed consolidation programs consistently report three benefits: reduced total cost of ownership, expanded recovery workload coverage (often revealing systems not previously protected), and materially improved incident response speed. Consolidation is not an end state in itself; it is the leveraged platform that makes genuine resilience possible.

Observation 1: Value Creation Opportunities

- Reduced total cost of ownership
- Expanded coverage across recovery workloads
- Complexity reduction
- Increased incident response and recovery speed
- Enhanced resilience risk reduction

RETURN TO TOC

Observation 2: The RTO/RPO Reality Gap – Recovery Objectives Require Empirical Validation

The second significant observation is the degree to which Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), widely cited in board-level reporting and regulatory submissions, have not been truly tested against real infrastructure under cyber-specific conditions.

These figures exist in disaster recovery documentation, but in many cases have not been tested on an empirical basis. This represents one of the clearest opportunities for resilience strengthening available to enterprise leadership today.

What the Data Shows

The underlying dynamic is consistent across sectors: standard RTO/RPO frameworks were designed for hardware failures and natural disasters—scenarios with a known, contained blast radius. Cyber incidents, in contrast, operate on different parameters putting traditional testing and validation approaches to the test: data may be corrupted rather than just unavailable, and recovery sequences must account for potential re-infection vectors.

Identity infrastructure is frequently compromised as part of the attack chain, creating dependencies that traditional recovery approaches do not accommodate. Rubrik Zero Labs research has found that 90% of IT and security leaders surveyed believe that identity-driven cyberattacks are the top threat to their organizations.

Airline Industry Example

In the airline industry, recovery metrics were understood to entail an RTO of 60 minutes and a RPO of 15 minutes. However, after testing, the actual estimated recovery time was revised to 4–5 hours of data loss and approximately one week for full, manual recovery. The gap between perception and reality is not incremental. It is an order of magnitude.

In practice, the gaps were stark: recovery plans untested against real-world scenarios, no measurement of RTO or RPO, and little recognition that a single cyber-driven outage can cascade far beyond the initial point of failure, disrupting downstream businesses and the customers they serve.

Untested recovery objectives don't just create false confidence—they create real operational and business risk. When plans are never stress-tested against realistic conditions, actual recovery times routinely overshoot targets, turning manageable incidents into major disruptions. The financial consequences compound quickly: lost revenue, inflated recovery costs, regulatory penalties, and productivity losses that were never budgeted for.

The Opportunity Forward

Organizations that treat recovery objectives as living, empirically-tested commitments rather than documented targets develop a qualitatively different resilience posture as a result.

Organizations need the ability to test recovery at scale without being operationally disruptive to the overall business, such as tooling to simulate recovery without impacting production environments. Secondly, insights from understanding current maturity levels and recovery objectives need to be leveraged to drive behavioral change.

The leading practice is to model recovery timelines using actual infrastructure data: backup set counts, system interdependencies, identity recovery sequences, and hydration rates. This produces metrics that credibly reflect true recovery capabilities and surfaces specific investments most likely to close the gap between stated and demonstrated resilience.

Observation 2: Value Creation Opportunities

- Increased confidence in recovery time and point objectives
- Improved predictive capabilities to plan for expected business disruption
- Planned costs of revenue impact during a major downtime or cyber driven event

RETURN TO TOC

Observation 3: Tier 0 and Tier 1 Infrastructure Recovery – A Significant Opportunity for Advancement

The third observation is that the organizations are largely unable to predict recovery timelines for their most critical infrastructure with confidence. Across more than 90% of field engagements, organizations had not yet established this capability for their most operationally critical infrastructure.

This is not a peripheral concern—Tier 0 and Tier 1 systems represent the foundational layer of enterprise operations: Active Directory, identity platforms, core databases, and ERP systems.

When these fail, everything fails.

What the Data Shows

For those engaged, identity infrastructure was the highest area of recovery concern. Identity can serve as the most critical Tier 0 application that underpins the critical infrastructure of an organization.

In significant ransomware incidents recently documented, Active Directory and identity management systems were targeted early in the attack chain because compromising or controlling identity enables an attacker to persist, escalate privilege, and re-establish access even after initial containment efforts.

Automobile Industry Example Scale of the Recovery Challenge

Processing ~1,800 backup sets per day, at an estimated 30 minutes per recovery set, would have cost one automotive organization approximately 38 days to conduct a full sequential recovery. This figure, derived from the organization's own infrastructure data, immediately reframes the conversation from cost-per-backup to business continuity risk.

At one large European bank, for example, analysis revealed a potential seven-day window to restore core Active Directory functionality, followed by an additional 120 or more days to fully remediate and validate identity infrastructure. This is not an outlier. It reflects the structural complexity of modern enterprise identity environments and the absence of purpose-built identity recovery tooling.

The challenges organizations face include false confidence in recovery, since the impact of extended downtime of Tier 0 and Tier 1 cascades across the business. A crisis scenario often uncovers undocumented dependencies, sequencing issues, and operational confusion that testing would otherwise have surfaced.There is also heightened financial and regulatory risk, as many regulators, auditors, and cyber insurers increasingly expect organizations to meet recovery objectives.

The Opportunity Forward

A purpose-built approach to Tier 0 and 1 workload restoration, combined with data-driven recovery time modeling, gives security and IT leaders a credible, provable answer to the question “How long will it actually take us to recover,and how do we know the environment is clean?”

Organizations should both define their Tier 0 and 1 applications and regularly perform full recovery exercises to prove infrastructure can be restored within business-required recovery objectives. Measuring recovery performance only goes so far without including executives and business stakeholders in recovery exercises to validate operational readiness and business-decision making, not just technical recovery.

The goal is to understand which systems are on the critical path to operational restart, and to ensure that those systems have recovery capabilities proportionate to their business impact.

Observation 3: Value Creation Opportunities

- Increased recovery performance and business continuity confidence
- Higher operational efficiency by reducing manual efforts and unnecessary processes
- Increased regulatory and audit readiness
- Stronger financial resilience pertaining to recovery expectations

RETURN TO TOC

Observation 4: Cyber Resilience Ownership Is Assumed, Not Assigned

The most organizationally significant observation is the near-universal absence of accountable ownership for cyber resilience outcomes. Approximately 90% of organizations engaged had not yet established the governance structures required to fully activate their resilience investments.

This is one of the more instructive observations from the research, because it demonstrates that the primary constraint on cyber resilience maturity is not technology—it is the organizational structure needed to restore businesses to full operational status after a major downtime or cyber event.

What the Data Shows

Many organizations do not have a clearly defined cyber resilience owner because responsibility is spread across multiple functions. Assigning accountability becomes increasingly difficult when organizational structures separate security, infrastructure, and business continuity functions.

For those without an accountable leader, a consistent set of gaps emerges:

- No clear authoritative direction
- A lack of regular reporting on cyber resilience to the executive team and board
- No Target Operating Model (TOM) that defines how resilience is governed, measured, and improved on an ongoing basis
- Missing resilience-by-design principles embedded in architecture reviews, procurement governance, and change management processes
- A lack of a skills framework for the cyber resilience function, covering incident response, recovery orchestration, and post-incident forensics
- No tested, executable recovery playbooks—not theoretical documentation, but procedures that the team has exercised under simulated conditions

Banking Industry Example – Criticality of the ownership challenge

The absence of a single accountable cyber resilience leader at a large global bank exemplified the cyber resilience risks. Board-level focus existed, but true ownership and accountability did not. Strategy, operating model, and recovery playbooks had all splintered. The board was demanding near-zero RTOs no one in the organization was positioned to meet.

The absence of one or more of these elements does not indicate organizational immaturity in a broader sense. It reflects the fact that cyber resilience as a structured business discipline is relatively young. Cyber resilience has become a greater priority as ransomware and cyber attacks have increased, and now organizations must adapt their governance models and frameworks.

The Opportunity Forward

When senior leaders question who owns cyber resilience—and what the operating model looks like for delivering it—it frequently catalyzes both organizational clarity and investment prioritization. Furthermore, cyber resilience governance and accountability, once surfaced as a board-level conversation, tend to advance more quickly.

The best positioned organizations have cyber resilience blueprints, operating model templates, and accountability frameworks that translate a complex technical discipline into clear ownership, measurable outcomes, and metrics for tracking progression.

Technological investments in cyber resilience deliver their full return only when the operating model infrastructure exists to activate them. Organizations that establish clear ownership and cross-functional governance, and that embed resiliency-by-design into their architecture, are able to convert technology capabilities into demonstrable resilience.

Observation 4: Value Creation Opportunities

- Faster decision-making and coordination during downtime and cyber incidents
- More consistent recovery testing and preparedness
- Higher accountability for cyber resilience outcomes
- Continuous improvement and maturity growth potential of cyber resilience

RETURN TO TOC

Observation 5: AI has Outpaced Governance, and the Exposure is Largely Unquantified

More than 80% of organizations are actively seeking guidance on AI governance and execution, and it is not difficult to understand why. AI initiatives have proliferated faster than the frameworks designed to govern them.

The organizations best positioned to manage this risk are those doing two things simultaneously: building the governance infrastructure to deploy AI responsibly and extending their resilience frameworks to protect the new categories of critical data that AI creates and depends on.

What the Data Shows

The most consequential AI resilience problem facing enterprises today is not a technology problem—it is a governance problem.

A pattern from the research is consistent: AI ambition is high and execution is accelerating, with governance frameworks representing the primary development area. This is not a constraint unique to any organization; it reflects the pace at which AI capabilities have advanced relative to the enterprise governance infrastructure designed to support them.

Organizations that close this gap early will establish a lasting competitive advantage in their ability to deploy AI reliably and at scale.

Public Sector Example Criticality of the AI Governance Challenge

A public sector organization serving 65 million+ citizens had both the mandate and the motivation to deploy AI as backlogs grew and the pressure to modernize was real. Leadership had limited confidence in their ability to govern and monitor AI agents at scale given the high risk of potential impact; a rogue AI acting on behalf of a state, at volume, could generate a public crisis.

OBSERVATION 5: AI HAS OUTPACED GOVERNANCE, AND THE EXPOSURE IS LARGELY UNQUANTIFIED

RETURN TO TOC

Large organizations operate under a different set of stakes. The observations make clear that, at scale, AI resilience is not a cost conversation but a question of whether the business can withstand an unanticipated agent action.

The financial exposure here is measurable, but widely unquantified. The reputational consequences may not be as easily overcome as a standard business shutdown. At this level of intricacy, treating AI governance and cyber resilience as separate workstreams poses greater complexity and risk.

The Opportunity Forward

AI and cyber resilience are inseparable. Organizations deploying AI at scale are creating new categories of critical data assets—training sets, model weights, inference pipelines—that require the same resilience guarantees as core business data.

Organizations need a data security platform that is positioned to extend into AI data protection and governance, addressing a business need that will only grow as AI deployment scales.

Observation 5: Value Creation Opportunities

- Turn AI governance into a competitive advantage
- Own the convergence of cyber resilience and AI governance under one platform
- Limit the damage of a rogue AI by leveraging a cyber resiliency platform

RETURN TO TOC

Conclusion

The data tells a consistent, urgent story: enterprise and AI cyber resilience is at a structural inflection point.

Cyber threats and downtime carry quantifiable financial exposure, documented operational disruption, and measurable risk to business continuity. What these observations reveal is not a technology gap, but a governance and accountability maturity gap.

RTOs are being underestimated and productivity losses from unplanned downtime are not widely appreciated. These gaps persist not because leadership lacks the will to close them, but because no structured forum has yet forced the financial and operational consequences onto the same agenda.

Organizations that treat this moment as a governance inflection point, not a procurement cycle, stand to gain a durable competitive and risk advantage. When gaps in recovery capability, identity exposure, and governance accountability are quantified in terms of financial exposure, productivity loss, and regulatory consequence, the conversation shifts. Leaders now can reframe cyber resilience as a board-level financial and operational imperative based on the organization's own risk data.

The leaders who will define what "good" looks like in the next three years are the ones who have closed the distance between what they assume and what they can prove. The question now is whether leadership is willing to make resilience a measurable business outcome—not just a line item in a security budget.

About This Document

This white paper was produced by Rubrik's Value Economics team based on synthesis of 50+ c-level and senior account conversations conducted from June 2025 - April 2026. References include organizations in Retail, Banking, Airline, Manufacturing, Oil & Gas and Public Sector across EMEA, APAC, and Americas. All figures are derived from customer-provided data or direct engagement observations. This document is confidential.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik (NYSE: RBRK) the Security and AI company, operates at the intersection of data protection, cyber resilience and enterprise AI acceleration. The Rubrik Security Cloud platform is designed to deliver robust cyber resilience and recovery including identity resilience to ensure continuous business operations, all on top of secure metadata and data lake. Rubrik's offerings also include Predibase to help further secure and deploy GenAI while delivering exceptional accuracy and efficiency for agentic applications.

For more information please visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn.

Rubrik is a registered trademark of Rubrik, Inc. All company names, product names, and other such names in this document are registered trademarks or trademarks of the relevant company.