July 2026
White Paper
Sponsored by Commvault

Resilience Operations: The Discipline That Makes Readiness Provable

Phil Goodwin
Research Vice President,
Infrastructure Software Platforms,
Worldwide Infrastructure Research, IDC

Craig Robinson
Research Vice President,
Security Services, IDC

Frank Dickson
Group Vice President,
Security and Trust, IDC

Table of contents

Click any title to navigate directly to that page.

IDC opinion

The first quarter of 2026 marked a sea change in the cyberthreat landscape. A compression of the timeline from initial compromise to breach, driven by attackers using AI automation to find and weaponize weaknesses, outpaces traditional detection and response cycles.

The introduction of the superstore of vulnerabilities, as currently epitomized by Project Mythos, is shining a bright light on the potential vulnerabilities that organizations need to address in their digital infrastructure. Frontier AI models now have the context window and parameter depth to reason across the full complexity of a large network operating system codebase, surfacing interdependencies that experienced human researchers have historically missed. Currently, the volume of vulnerability disclosures has been accelerating for many years; leading-edge frontier models, however, can chain vulnerabilities together to create sophisticated exploits in hours, a task that once took years.

Vulnerability volume + complex exploit creation + speed = elevated threat

This framing is not marketing hyperbole. It reflects a genuine shift in attacker capability that IDC has been tracking across the vendor landscape. The practical consequence for enterprise security teams is that a historical "good enough" security and recovery approach is no longer a defensible posture. No organization, regardless of size, industry, or geography, is exempt. IDC's survey of 539 North American organizations found

that the plurality of respondents (33.8%) suffer between one and five attacks per year, while the industry-wide mean reaches 11.3 attacks annually across all attack types. The financial and operational stakes are rising accordingly.

Data protection and backup operations alone are insufficient to guarantee IT system recovery. The problem, IDC's research reveals, is largely structural: IT, security, and business functions have historically approached cyber-resilience from siloed perspectives, with no shared operating model, no common language, and no coordinated recovery strategy. The weakness in most organizations lies in the gaps between those functions, whereby activity between groups goes uncoordinated. Historically, only the most sophisticated adversaries could exploit these gaps. As frontier AI models become broadly accessible, even unsophisticated attackers can mount assaults with nation-state sophistication.

To address these gaps between functions, a new operating discipline is emerging: resilience operations, or ResOps. ResOps is not an IT function. It is a cross-functional framework that integrates cyber preparedness, infrastructure deployment, data protection, and disaster recovery capabilities with the business delivery requirements of the organization. The primary mission of a ResOps team is to maximize the business function availability, and in the event of a disruption, return it to its minimum viable business (MVB), the set of functions, processes, and systems required to serve customers and generate revenue, as quickly as possible.

The urgency of defining the MVB is underscored by a striking finding: More than half of the organizations surveyed (57.7%) have not fully defined their MVB. Without a clear, documented target for recovery, even the best-resourced IT teams are operating without a clear understanding of the objective.

This paper addresses three interconnected topics: the growing need for ResOps as a response to structural resilience failures; the principles and dimensions of MVB definition; and the IDC ResOps Maturity Model, a four-stage framework that enables organizations to assess their current state, identify gaps, and chart a measurable path toward operational resilience.

IDC perspective

ResOps brings together business, IT infrastructure, and incident response teams into a coordinated resilience discipline. The main charter of the ResOps team is to ensure the return of the organization to the MVB to minimize customer and organizational impact in the event of a cyberattack or other disruption. ResOps teams will evolve along a definable maturity curve, making progress predictable and measurable.

Study methodology

Commvault commissioned IDC to conduct a primary research study with the following objectives: to determine the current state of organizational resilience; to describe ResOps in practical, operational terms; to understand how organizations conceptualize and approach MVB recovery; and to define a maturity model for ResOps that identifies the steps organizations must take to achieve mastery.

To meet these objectives, IDC surveyed 539 North American organizations, with respondents drawn 80% from the United States and 20% from Canada. The sample was constructed to be representative of the broader market by organizational size and industry vertical. All participants held senior IT or C-level roles with substantive knowledge of and authority over their organization's resilience strategy and plans.

In addition to the quantitative survey, IDC conducted three in-depth qualitative interviews with resilience leaders at mid- to large-scale organizations. These interviews provided the depth of context necessary to interpret the quantitative data, surfacing the organizational dynamics, decision-making patterns, and implementation challenges that survey responses alone cannot fully capture.

Unless otherwise noted, all research referenced in this paper is from IDC's *Cyber Resilience Survey,* May 2026; n = 539.

Situation overview

Many vectors, one goal: The modern attack landscape

Modern cyberattacks are not monolithic events. They take many forms: distributed denial-of-service (DDoS) attacks, data exfiltration, data destruction, ransomware deployment, cloud-targeted intrusions, and combinations thereof.

IDC's survey data reveals that these attack modalities occur at roughly similar rates across the respondent population, a pattern that suggests attackers routinely deploy multiple techniques in parallel. The objective is not merely to succeed with one approach but to maximize leverage: staging simultaneous vectors to improve the likelihood of a ransom payment, enable multiple ransom demands, or complicate recovery so severely that victims capitulate.

AI also expands the disruption possibilities. AI-enabled development pipelines deliver application changes faster than traditional controls can validate them, and AI systems introduce entirely new failure modes, including model drift, training data poisoning,

and prompt exploitation, that neither traditional security tooling nor traditional backup practices were designed to detect or recover from. Resilience planning that accounts only for human-driven attack vectors will systematically underestimate the recovery scenarios the organization must be prepared to address.

Cyberattacks continue to carry significant stigma at the highest levels of the organization. Recovery from a major incident demands executive attention, draws regulatory scrutiny, and carries reputational consequences that extend well beyond the technical recovery itself.

Key findings: Data protection and recovery

IDC's survey surfaced six critical findings related to data protection and recovery posture across the surveyed population. Together, they reveal a market in which critical foundational capabilities remain broadly underdeveloped despite years of increased investment in cybersecurity.

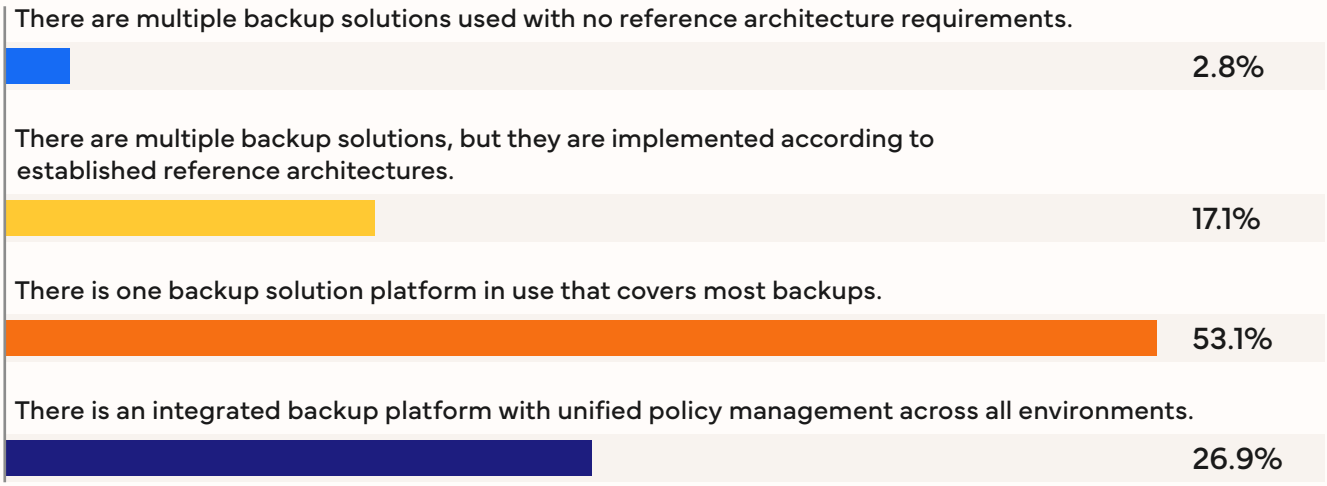
Finding 1: Most organizations lack a unified backup platform

Only 26.9% of respondents report having an integrated backup platform with unified policy management across their organization (Figure 1, below). For three out of four organizations, data protection exists in the form of multiple, fragmented backup products with separate policy engines, a configuration that produces recovery silos, inconsistent retention and protection policies, redundant operational overhead, and substantially longer recovery timelines. A single, unified backup and policy platform that provides full visibility into the recovery posture across the application estate reduces or eliminates these inefficiencies and is a prerequisite for rapid MVB recovery.

Figure 1

Unified backup deployments

(Percent of respondents)



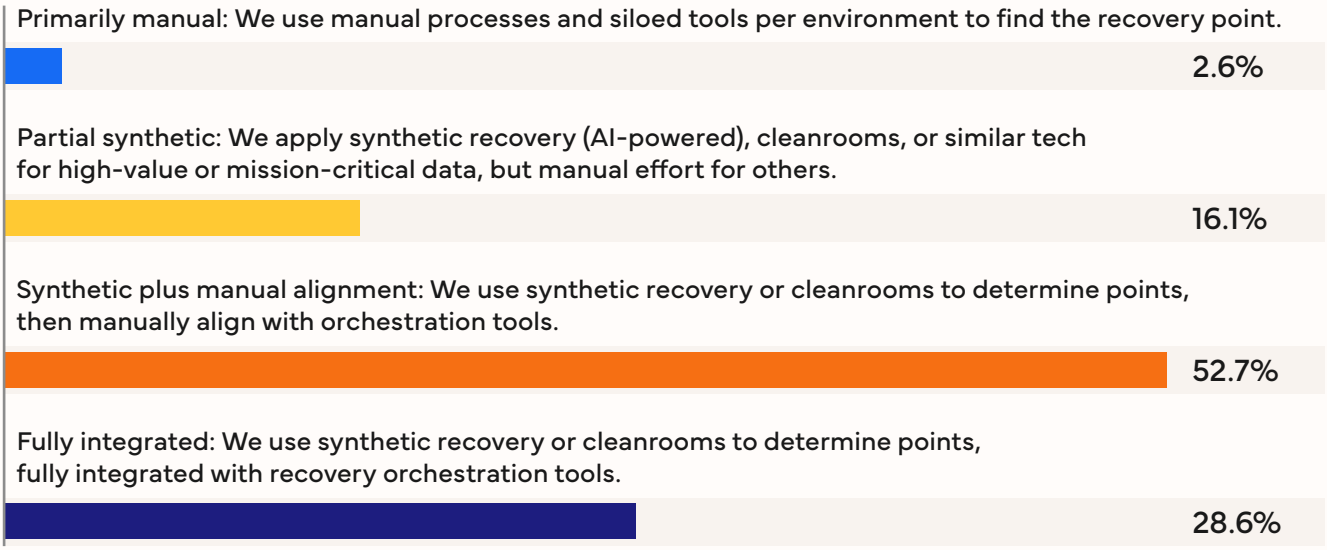
Finding 2: Automated clean recovery points remain the exception

Only 35.4% of respondents have implemented automated clean recovery point identification using automated orchestration (Figure 2, below). Modern cyberattacks are asynchronous by nature: They compromise different systems at different times, through different methods, and often without leaving a single identifiable clean point of recovery across the environment. There is rarely a single moment when the whole environment was last known to be clean and healthy, so recovery becomes less like rewinding a tape and more like reassembling a document from many differently dated drafts. Identifying clean recovery points for potentially hundreds or thousands of file systems and databases is an enormously time-consuming task when performed manually. Organizations that have automated this process save days or weeks of recovery time relative to those that have not.

Figure 2

Recovery point determination

(Percent of respondents)

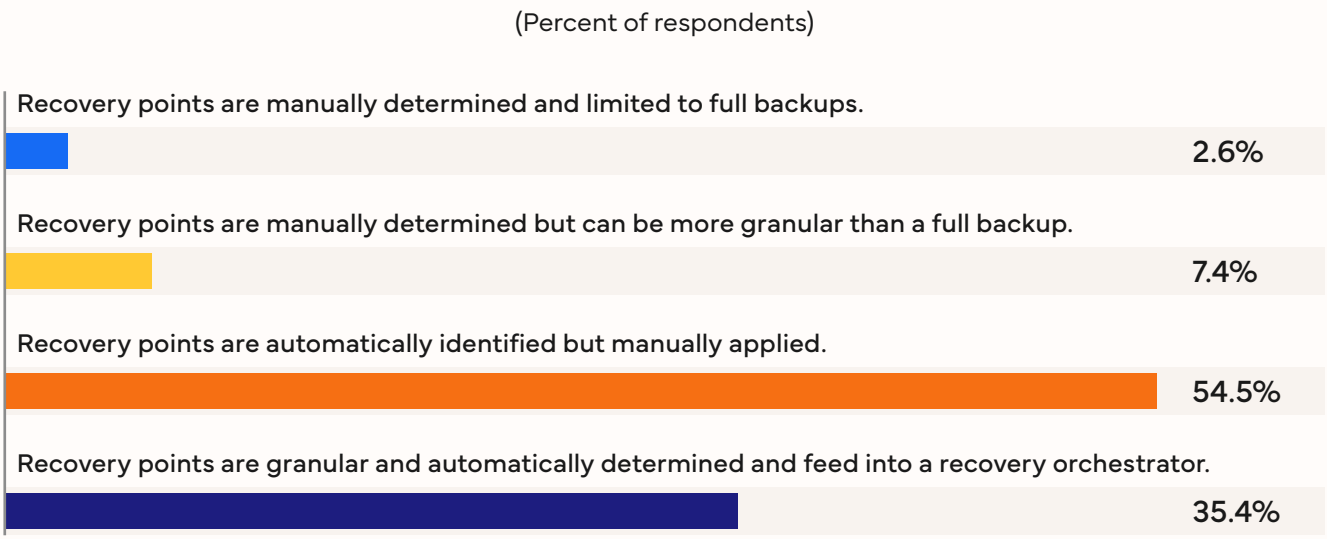


Finding 3: The majority of organizations have limited automated recovery point determination and recovery orchestration

More than 64% of respondents indicate that their recovery point determination requires manual intervention and is not integrated with recovery orchestration capabilities (Figure 3, below). Manual recovery processes are not only slow; they are also error-prone. Recovery orchestration platforms can optimize recovery sequences, enforce prioritization against MVB criteria, and reduce the risk of human error at precisely the moment when organizational stress is highest. The absence of orchestration is among the most significant contributors to extended recovery timelines. AI-driven recovery orchestration leverages even greater automation for recovery at scale.

Figure 3

Recovery point determination and orchestration integration



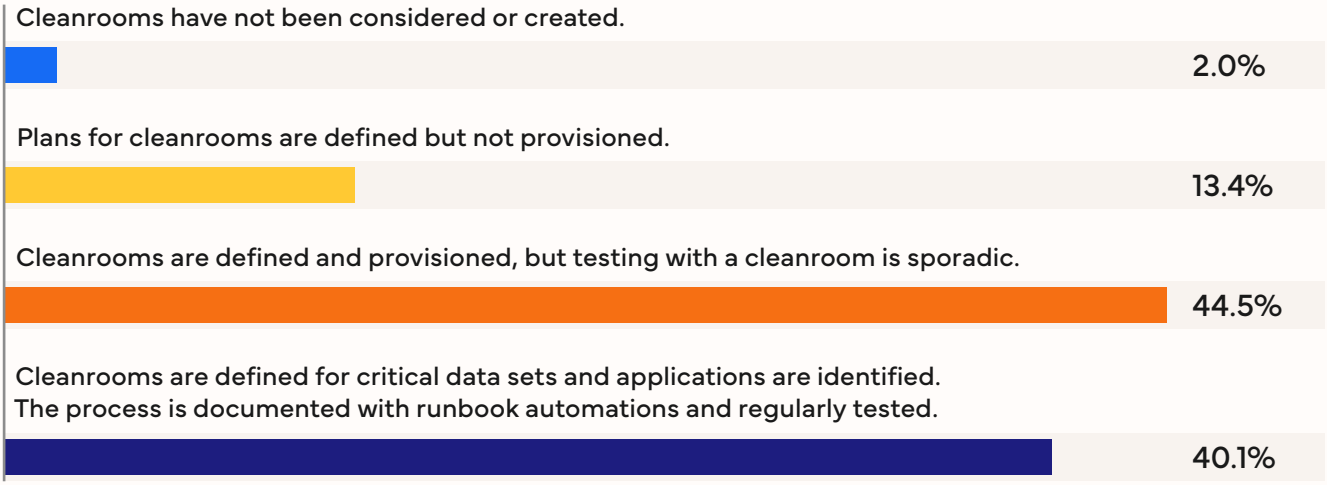
Finding 4:
Cleanroom implementations are widely absent

More than 59% of respondents have limited or no cleanroom implementations (Figure 4, below). Cleanrooms, isolated infrastructure environments used to stage recoveries, conduct forensic analysis, and scan data for malware before recovery, are a critical safeguard against reinfection. Without a cleanroom, organizations that recover directly into their production environment face a substantially elevated risk of reintroducing malware that was not identified during the initial response. Recovering straight into production without a cleanroom is like performing surgery without sterilizing the instruments first: The procedure may succeed while quietly reintroducing the original infection.

Figure 4

Cleanroom implementations

(Percent of respondents)



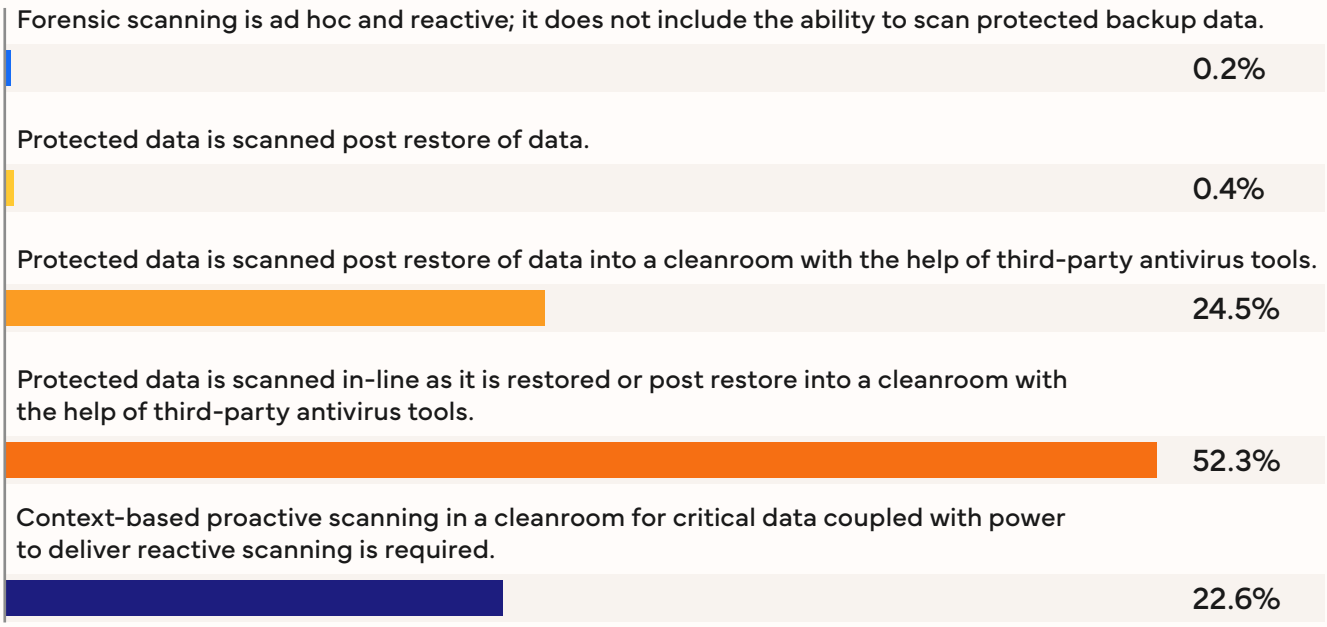
Finding 5: Context-based scanning is rarely deployed

Only 22.6% of respondents have deployed context-based scanning (Figure 5, below). Context-based scanning uses behavioral and semantic analysis to identify malware more accurately than signature-based approaches, and it is most effectively applied within a cleanroom environment to validate recovery candidates before they are reinstated to production. Relying on older signature-based approaches may allow newer, more targeted malware to slip through.

Figure 5

Cleanroom deployments with context-based scanning

(Percent of respondents)



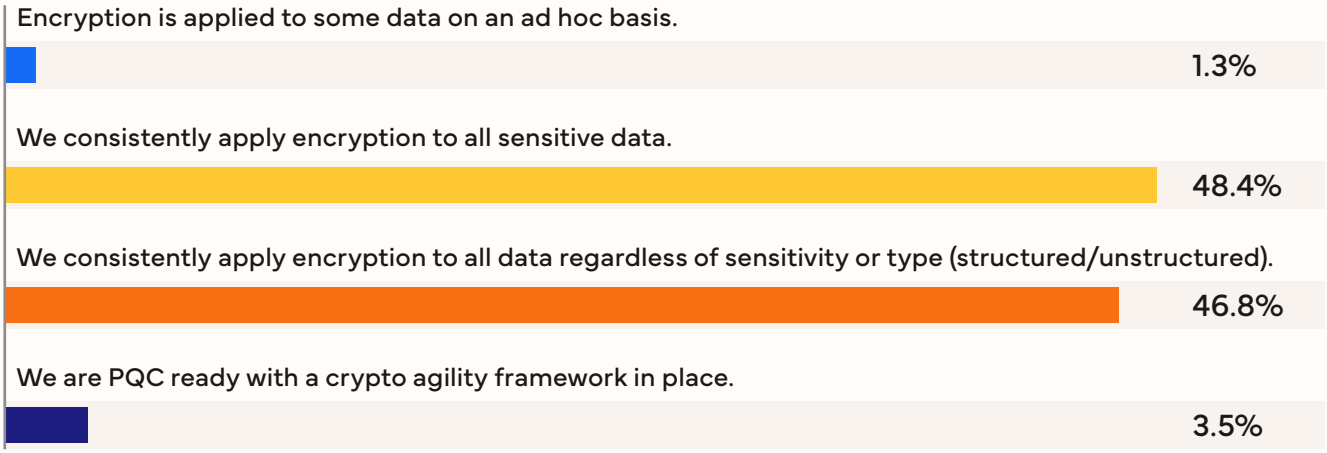
Finding 6: The post-quantum cryptography gap is severe

Only 3.5% of respondents report that their organizations are post-quantum cryptography (PQC) ready, despite growing evidence that the timeline for quantum-related cybersecurity risks is compressing (Figure 7,below). While today's classical computing systems require an impractical amount of time to compromise data protected by modern cryptographic standards, rapid advances in quantum hardware, quantum error correction, and algorithmic resource optimization are increasing confidence in the feasibility of large-scale fault-tolerant quantum computing. Recent developments across the industry support this view. IDC believes enterprises should prepare for the possibility that quantum systems capable of compromising certain widely deployed public-key cryptographic algorithms may begin to emerge as early as 2030. This compressed timeline increases the urgency of addressing "steal now, decrypt later" risks, in which adversaries potentially collect and store encrypted information today, expecting to decrypt it once sufficiently powerful quantum systems become available. Post-quantum cryptography provides a standardized set of quantum-resistant algorithms designed to protect sensitive data at rest and in transit against both current and future quantum-enabled threats.

Figure 6

Post-quantum cryptography (PQC) readiness

(Percent of respondents)



Key findings: Data security

Almost everyone agrees, and that is the story: Collaboration failures

Almost all (98.4%) of respondents expressed the need for better collaboration between the teams responsible for IT security. Near-unanimity of this magnitude is exceptional in broad-sample research. It signals not merely a widespread preference but an acute, broadly shared recognition that siloed security operations are increasing organizational risk.

More machines than people: Agentic AI and identity management

The majority (90.3%) of respondents believe their organizations need to improve identity management practices in response to the risks introduced by agentic AI systems. As organizations deploy AI agents at scale, the number of non-human identities in the environment can quickly exceed the total number of human users. Identity systems built to manage a roster of employees suddenly have to govern

a population of AI agents that have persistent access and multiply on demand. IDC also recognizes that many of these new machine identities are built or cloned from their human counterparts, which are often already over-permissioned.

Nearly two-thirds of respondents (58.7%) indicated a need for "significant improvements" or "a complete overhaul" of their identity management capabilities.

Rehearsal predicts performance: Testing cadence

Only 28.9% of respondents conduct more than one tabletop exercise or cyber-range recovery simulation per year. Regular testing is the single most reliable predictor of recovery performance under real incident conditions. Best practice organizations conduct these exercises semi-annually or quarterly, recognizing that while this requires a large amount of time and resources to properly rehearse, the benefit is that good practice habits foster better results when needed in an actual attack. Indeed, testing is not about passing the test per se; it is about identifying weaknesses and fostering continuous improvement.

IDC notes that the majority of organizations in the survey are well below this standard.

Visibility you are not yet using: Data security posture management as a resilience signal

Only 24% of respondents use data security posture management (DSPM) as a live resilience signal. DSPM is a cybersecurity capability that continuously discovers sensitive data, assesses its risk exposure, and monitors for misconfigurations or policy violations in real time. The majority of organizations surveyed are not yet operating at this level of continuous visibility. Although many organizations have DSPM tools, not using them as a resilience signal is a missed opportunity for greater protection.

Future outlook

A structural problem needs a structural fix: Defining ResOps

The findings presented in the previous section paint a consistent picture: Organizational resilience is impaired not only by gaps in individual technologies but by the absence of a coordinating framework that brings business, infrastructure, and security functions together around a shared recovery objective. **ResOps is that structural solution.**

IDC defines the discipline as follows:

- ResOps is a continuous, operational discipline that integrates cyber-preparedness, infrastructure deployment, data protection, and disaster recovery practices with business delivery requirements to return a company to an operational state following business-disrupting events.

The definition is precise on two points that distinguish ResOps from earlier models of cyber-response. First, it is continuous: not a project, a plan, or a post-incident response; but an ongoing discipline embedded in the organization's operating model. Second, it is explicitly anchored to business delivery requirements. The return to an operational state is not defined in purely technical terms but in business terms: Is the organization able to serve its customers and generate revenue at normal or near-normal levels?

Mature ResOps is distinguished by proof of effectiveness. Resilience plans that exist only on paper have no assurance of success under the stress of cyberattack. Mature ResOps organizations validate recovery plans and prove readiness through testing and telemetry, so leadership can be confident of maintaining a viable business. While cyberattack is the forcing function driving ResOps adoption, the discipline applies to the full spectrum of business-disrupting events, including data corruption, third-party and SaaS provider failure, cloud region outages, loss of key personnel, physical events, and compromise of AI systems.

The floor you cannot fall below: The minimum viable business

The MVB is the smallest complete set of functions, processes, systems, and data required to serve customers and generate revenue, the operational floor below which the organization cannot sustain itself as a going concern. MVB is not the same as full operational restoration; it is the target state that allows the business to function while complete recovery proceeds in parallel. It is the corporate equivalent of Apollo 13's "what do we need to get them home" list, the short inventory of systems that must come back before anything else does.

During in-depth interviews conducted as part of this research, resilience leaders revealed the degree of difficulty involved in defining the MVB in practice. For some organizations, the MVB encompasses as much as 80% of the application catalog. When the vast majority of their digital infrastructure is classified as critical, organizations must be cautious of setting impossible all-or-nothing recovery options. Difficult choices are required when defining what is truly critical to a functioning organization.

In no case were interview participants able to assign a definitive service-level agreement (SLA) to MVB recovery because the recovery timeline is necessarily a function of the nature and extent of the disruption.

IDC recommends that organizations approach MVB scoping across five dimensions:

- **Revenue criticality:** Which processes directly generate or protect revenue, and which customer-facing functions are essential to maintaining commercial relationships?
- **Regulatory and compliance obligations:** What are the non-negotiable legal minimums that must be maintained even during a recovery period?
- **Customer experience thresholds:** What minimum service-level commitments to customers must be honored to avoid material reputational or contractual harm?
- **Employee productivity baselines:** What tooling, access, and systems do employees require to perform the functions that support the MVB?
- **Security and risk posture:** What minimum controls must remain operational to prevent a secondary breach or escalation during the vulnerability of a recovery period?

The IDC ResOps maturity model

Based on IDC's survey of 539 North American organizations and in-depth interviews with resilience leaders, organizations can be grouped into four distinct stages of ResOps maturity. These stages represent definitive milestones along the journey from ad hoc, siloed cyber-response toward a fully integrated, continuously improving resilience discipline.

The model is anchored by a defining principle: the ability of an organization to return to its minimum viable business as quickly as possible following a cyberattack or other disruption. An organization's stage of maturity directly predicts how well it can define, plan for, and prove MVB recovery **(Figure 8, below).**

Figure 7

IDC ResOps maturity model: Four stages of resilience operations advancement

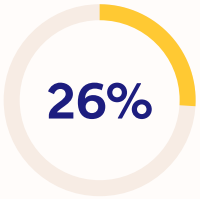
Stage	Stage name and descriptor
Stage 1	Reactive: Siloed and uncoordinated
Stage 2	Aware: Visibility and early alignment
Stage 3	Coordinated: Governed and tested
Stage 4	Resilient: Optimized and adaptive

Source: IDC, 2026

Stage 1
Reactive: Siloed and uncoordinated

Organizations at the Reactive stage treat cyber-response as a problem belonging to a single team, most often the security operations center or the IT infrastructure group, rather than as an enterprise-wide discipline. Data protection exists in the form of backup tools, but those tools are siloed across business units with inconsistent policies and no unified management plane. When an attack occurs, recovery is manual, reactive, and dependent on the heroic efforts of individuals rather than on repeatable, documented processes.

The concept of a minimum viable business is largely undefined at this stage. Leaders may have an intuitive sense of which systems are most important, but that understanding has not been formalized, documented, or translated into specific recovery priorities.



of organizations have an integrated backup platform with unified policy management — meaning three out of four operate with the fragmented, siloed data protection that is the hallmark of Stage 1.

Organizations at Stage 1 are characterized by:

- Backup platforms fragmented across business units, with inconsistent retention and policy management
- Business disruption tolerances that are undefined or expressed only as technical RTO/RPO metrics disconnected from business consequences
- Recovery orchestration absent or entirely manual, relying on tribal knowledge
- No cleanroom or isolated recovery environment; recoveries performed directly in production
- Limited or no tabletop exercises or cyber-range testing
- No documented MVB definition; recovery priorities determined ad hoc during incidents
- Identity and access management not adapted for agentic AI risks or modern attack vectors
- No assurance for organizational leaders regarding business continuity and recovery to a viable state

The business consequences of operating at Stage 1 are severe. Without a defined MVB, and without the coordination structures to pursue it, recovery timelines extend from days into weeks. Revenue impact compounds with each hour of downtime. Customer trust erodes. Regulatory exposure accumulates.

Stage 2
Aware: Visibility and early alignment

Aware organizations have recognized the inadequacy of their siloed approach and have begun the structural work of alignment. IT leadership has initiated conversations across security, infrastructure, and in some cases, business unit functions about what a coordinated response model could look like. An informal ResOps working group may exist, though it typically lacks an executive mandate, dedicated budget, or formal enforcement authority.

At this stage, organizations begin taking inventory of their backup and recovery tooling, their application catalogs, and the critical dependencies between business processes and the systems that support them. This inventory work is the prerequisite for MVB definition.

Organizations at Stage 2 are characterized by:

- An informal cross-functional working group discussing resilience operations
- Initial efforts to consolidate or standardize backup platforms across business units
- Early-stage MVB scoping underway, typically involving IT and select business unit leaders
- Initial dependency mapping underway for candidate MVB components, spanning applications, data, infrastructure, third parties, and key personnel
- Draft business impact thresholds proposed for the most critical business functions, though not yet validated through testing
- Some recovery orchestration tooling deployed but not consistently used across the environment
- Cleanroom capabilities under evaluation or in initial deployment for a subset of workloads
- Tabletop exercises conducted once per year or less
- Identity management improvements initiated but not systematically enforced

The Aware stage is defined by momentum, not completion. The transition from Aware to Coordinated requires executive commitment to formalize what the working group has started. Proof of recovery capability is not yet achieved.

Stage 3
Coordinated: Governed and tested

Coordinated organizations have made the structural commitments that transform resilience from an aspiration into an operational discipline. A formal ResOps function exists with executive sponsorship, typically at the CIO and CISO levels, and with defined membership spanning IT infrastructure, security operations, application teams, and business unit representatives. The ResOps charter includes authority over recovery prioritization and the ability to enforce policy adherence across functions.

The MVB has been formally defined at Stage 3. Business unit leaders have participated in scoping exercises to identify the critical processes, applications, and data sets that constitute the minimum viable business. SLA commitments, including recovery time objectives (RTOs), recovery point objectives (RPOs), and mean time to viable business (MTVB), are mapped to individual MVB components, not merely to individual systems.

Organizations at Stage 3 are characterized by:

- A formal ResOps function with executive sponsorship and cross-functional membership
- A documented MVB definition, mapped to specific applications, data sets, business processes, facilities, key personnel, and third parties
- SLAs assigned to MVB components, with RTOs and RPOs defined at the business capability level with business unit involvement to align with MTVB
- Automated recovery orchestration deployed and regularly exercised across critical workloads
- Cleanroom environments operational for staged recovery, forensic analysis, and malware scanning
- Tabletop or cyber-range exercises conducted semi-annually or quarterly, mapped to the risk management profile
- Context-based scanning deployed to identify malware in recovery candidates before reinstatement
- DSPM implemented as a real-time resilience signal
- A defined transition plan between business-as-usual operations and crisis operations, with explicit decision trees and role descriptions and responsibilities

IDC perspective

Coordinated organizations have crossed the most consequential threshold in the ResOps maturity journey: They have translated executive intent into operational structure. The MVB definition, in particular, represents a forcing function that requires business leaders and IT leaders to agree on what actually matters and to commit those priorities to writing before an incident makes the decision for them.

Coordinated organizations recover from cyberattacks with dramatically greater speed and consistency than their Stage 1 and Stage 2 counterparts. The combination of defined MVB priorities, automated orchestration, cleanroom infrastructure, and regular testing creates a resilience system that performs under pressure because it has been designed, and rehearsed, for that purpose.

Stage 4
Resilient: Optimized and adaptive

Resilient organizations represent the apex of ResOps maturity. They have not only built the governance, technical, and operational foundations of a coordinated resilience discipline; they have embedded continuous improvement into the operating model itself. The ResOps function at this stage is a recognized strategic capability, resourced and valued at the executive level alongside other core enterprise disciplines.

The MVB is treated as a living document, recalibrated quarterly in response to shifts in business strategy, application portfolio changes, regulatory developments, and the evolving threat landscape. AI-assisted tooling supports real-time monitoring of resilience posture; automated detection of clean recovery points across complex, asynchronous attack scenarios; and predictive modeling of recovery timelines.

Post-quantum cryptography is on the active roadmap of Resilient organizations. With quantum computing capabilities projected to render current key encryption vulnerable by 2030, and with attackers already executing "steal now, decrypt later" strategies against high-value targets, organizations at this stage are implementing quantum-resistant encryption for data at rest and in flight.

Organizations at Stage 4 are characterized by:

- ResOps recognized as a strategic enterprise capability with dedicated budget and executive visibility
- Documented recovery evidence that drives investment prioritization, change approval, vendor selection, and board-level risk decisions
- MVB definition continuously maintained and re-validated against evolving business and threat conditions driving technology choices and impact expectations
- AI-assisted clean recovery point identification, automated across hundreds of file systems and databases
- Synthetic recovery fully implemented with automated orchestration, enabling complete environment recovery
- Cyber-range exercises conducted quarterly, with results systematically integrated into recovery playbooks
- DSPM functioning as a live resilience signal, surfacing misconfigurations and anomalies in real time
- Identity management adapted for agentic AI at scale, governing both human and non-human identities
- PQC implementation underway or complete for high-value data assets
- ResOps KPIs integrated into executive reporting, board-level risk disclosures, and objectives and key results (OKR) frameworks

Key insight: No organization starts at Stage 4

Not all organizations begin at Stage 1, but none begin at Stage 4. The IDC ResOps Maturity Model provides a structured framework that helps CIOs, CISOs, and operational leaders identify where their organization stands and determine the highest-impact actions to advance to the next stage. The journey is achievable, and progress is measurable.

Where most organizations stall: Advancing through the stages

The transition between maturity stages is not automatic. Each stage transition requires deliberate action across three dimensions: organizational structure (governance, charters, accountability), technical capability (tooling, automation, testing infrastructure), and operational practice (defined processes, SLAs, continuous improvement mechanisms). Organizations that attempt to advance technical capability without the corresponding governance and process maturity often find that their investments underdeliver.

IDC's research consistently identifies the transition from Stage 2 to Stage 3 as the most common stall point in the ResOps maturity journey, the passage from informal alignment to formal governance. This transition requires executive commitment to fund and charter the ResOps function and active participation from business unit leaders in the MVB scoping process. It is also the point at which the organization's basis for confidence must shift from plans to proof, and that shift cannot be purchased; it must be governed.

The maturity journey is neither purely sequential nor uniformly paced. Organizations may advance specific technical capabilities, cleanroom deployment for example, ahead of their overall governance maturity, and they may accelerate their progress in response to an incident that clarifies the cost of resilience gaps.

Implementing ResOps: A practical roadmap

Translating ResOps from a conceptual framework into operational reality is a phased undertaking. IDC's research identifies four implementation phases that correspond to progressive levels of organizational and technical maturity. Each phase builds on the prior, and the sequencing reflects both practical dependencies and organizational change management realities.

Phase 1: Foundation

The foundation phase is primarily organizational and discovery-oriented. Its purpose is to establish the governance structures and knowledge base that all subsequent activity will depend on.

Key activities include:

- Establishing a ResOps steering committee with explicit executive sponsorship from the CIO, CISO, and COO, along with other relevant executives
- Conducting a comprehensive inventory of technology assets, licenses, and human capacity across the enterprise
- Deploying or activating tooling for cost and resource visibility, including FinOps platforms, configuration management database (CMDB) refresh, and capacity management instrumentation
- Conducting dependency mapping for the initial MVB scope, identifying the applications, data stores, infrastructure, identities, third parties, and key personnel that each business-critical function requires
- Defining the initial MVB scope for the top three to five business-critical domains using the five-dimension framework described earlier in this paper
- Appointing a resilience operations leader, a head of ResOps or equivalent, reporting to senior management

Phase 2: Governance and policy

With foundational visibility established, Phase 2 is focused on translating that visibility into governance, the formal structures, policies, and accountability mechanisms that give ResOps its operational force.

Key activities include:

- Defining resource and capability tiering: Tier 1 (MVB-critical), Tier 2 (strategically important), and Tier 3 (discretionary)
- Establishing allocation policies, approval workflows, and escalation paths for recovery prioritization
- Integrating ResOps metrics into executive reporting cycles and organizational OKR frameworks
- Piloting ResOps governance in one business unit, documenting learnings, and refining the model before enterprise-wide rollout

Phase 3: Optimization and scaling

Phase 3 extends the governance model established in Phase 2 across the full enterprise and begins introducing automation and intelligence to reduce human dependency in recovery operations.

Key activities include:

- Extending ResOps governance across all major business units, applying lessons from the Phase 2 pilot
- Introducing AI-assisted anomaly detection and demand forecasting to enable proactive resilience management
- Automating routine recovery validation and recovery sequencing decisions within defined policy guardrails
- Publishing ResOps dashboards that score recoverability posture, test results, and resilience gaps, linked with business outcome indicators

Phase 4: Continuous improvement

Phase 4 is not a discrete project phase but an embedded operating practice.

Key activities include:

- Recalibrating MVB quarterly in response to business strategy shifts, application portfolio changes, and threat landscape developments
- Regularly benchmarking resilience performance against the IDC ResOps Maturity Model
- Cultivating a ResOps community of practice across the enterprise to share learning, identify emerging risks, and propagate best practices
- Operating of a continuous feedback loop in which exercises, drills, and incident response results are shared with stakeholders and used to improve ResOps to facilitate ongoing maturity

Technology enablers for ResOps

No single platform does it all: The ResOps tooling landscape

Effective ResOps implementation requires a coordinated ecosystem of enabling technologies.

No single platform addresses the full scope of ResOps requirements; rather, a well-integrated set of capabilities across the following categories is needed:

- Data protection platforms with unified orchestration and governance spanning backup, recovery, and retention policy management across the enterprise
- Alternative and air-gapped infrastructure for isolating critical workloads and maintaining recovery capability in adversarial conditions
- Cleanrooms, cybervaults, and forensic analysis environments for staged recovery, malware scanning, and incident investigation
- DSPM and cyber risk quantification (CRQ) tools to continuously assess data security posture and translate security gaps into business risk terms
- Malware detection and remediation tools, including endpoint detection and response (EDR), extended detection and response (XDR) platforms, for identifying and containing threats before and after recovery
- AIOps and observability platforms that provide real-time resource telemetry and anomaly detection across the production environment
- IT service management (ITSM) and CMDB platforms for configuration management, dependency mapping, and change tracking
- Security information and event management (SIEM) tools for cybersecurity to aggregate, analyze, and correlate log data across an organization's network to detect threats and manage security incidents
- Incident response (IR) and security orchestration, automation, and response (SOAR) tools for orchestration and the coordination of cross-functional response activities during and after an attack

IDC recommendations

ResOps succeeds or fails on whether leaders across the organization act on it, so the guidance below is grouped by the role best positioned to drive each commitment. The recommendations build on the maturity model: They describe the deliberate steps that move an organization from a reactive, siloed response toward a coordinated, tested discipline. No single function can deliver resilience alone, which is why the actions span technology, finance, and business leadership.

For CIOs, CTOs, CISOs, CROs, and other technology leaders

- Establish ResOps as a strategic operational capability, not an IT cost-cutting initiative or a compliance exercise, with its own governance structure, executive sponsorship, and budget.
- Mandate MVB scoping as a required component of annual business continuity and IT planning cycles, ensuring that the definition is validated against the current business strategy each year.
- Invest in tooling that provides real-time, cross-domain resource and resilience visibility.
- Build a ResOps center of excellence to develop and maintain recovery standards, document institutional learning from exercises and incidents, and propagate best practices across business units.

For CFOs and finance leadership

- Align the technology investment taxonomy with business capability tiers as defined in the MVB.
- Require ResOps performance metrics in technology spend reviews and board-level risk reporting, treating resilience as a measurable financial risk management capability rather than a cost center. Certify that technical resilience findings are translated into customer, financial, and regulatory compliance within the context of enterprise risk.
- Use the delta between current operating cost and MVB-level operating requirements as an input into economic downturn and crisis scenario planning.

For operational and business unit leaders

- Participate actively in MVB scoping exercises to ensure that the critical capabilities of your business unit are accurately represented.
- Champion resource and resilience transparency within your business unit, and treat ResOps KPIs as leading indicators of operational health rather than as compliance metrics.
- Support regular tabletop and cyber-range exercises as investments in organizational capability, not interruptions to business operations.

Challenges and opportunities

Recommendations describe the destination. Reaching it is another matter. The organizations that adopt ResOps successfully are not the ones that buy the most tooling; they are the ones that anticipate the friction the discipline creates and plan for it. The obstacles below are predictable, and naming them in advance is the first step toward managing them.

Organizational and cultural barriers

- **Resistance to transparency:** ResOps programs surface inefficiency, redundancy, and gaps that were previously invisible or tolerated.
- **Siloed ownership models:** Teams that have long owned their own recovery and resilience processes may resist the cross-functional governance that ResOps requires.
- **Skills gaps:** Effective ResOps implementation requires capabilities in data analysis, resilience engineering, and business continuity planning that may not currently exist in sufficient depth.

Technical and data challenges

- **Incomplete or inaccurate asset inventories** that undermine the accuracy of MVB scoping and recovery baseline assessments
- **Shadow IT and unmanaged SaaS deployments** that create blind spots in the protection and recovery landscape
- **Integration complexity across heterogeneous tool landscapes** that have accumulated through years of independent procurement decisions

Ecosystem risks

- **ResOps is not a product for purchase.** Even when it comes to the technology aspects, no single company can supply all of the components needed to implement it.
- **ResOps will evolve rapidly,** not just with technology, but as the threat landscape evolves. Success will require continual attention and change.

Conclusion

Organizational resilience in the face of cyberattacks requires more than backup infrastructure. It requires a coordinating framework that unites business, infrastructure, and security functions around a shared, defined, and continuously maintained recovery objective. That framework is ResOps. That objective is maximizing business operating uptime and maintaining at least the minimum viable business.

The IDC survey of 539 North American organizations reveals a market in which the structural prerequisites for effective cyber-recovery are broadly underdeveloped: Most organizations lack unified backup platforms, automated recovery orchestration, cleanroom environments, and, most fundamentally, a formally defined MVB. These are not technological limitations. They are governance and organizational design failures that ResOps is specifically designed to address.

The IDC ResOps Maturity Model provides a structured pathway from the reactive, siloed posture that characterizes most organizations today toward the optimized, adaptive discipline of Stage 4 Resilient organizations. The journey is achievable, and progress is measurable. But the cost of delay is not abstract. The consequences compound with each hour of extended recovery and each reinfection that follows an inadequately validated restoration. They compound again with every data set an attacker captures today, betting that quantum computing may strip its encryption as early as 2030. Resilience is the insurance an organization buys before the fire, not the hose it reaches for after the building is already alight.

IDC predicts that ResOps will mature from an emerging discipline into a mainstream enterprise capability over the next three to five years. Organizations that build the governance structures, technical capabilities, and testing disciplines now, before the next major incident, will be better positioned to absorb disruption, protect their customers, and sustain competitive operations in an increasingly hostile threat environment.

Appendix

This appendix provides the findings from select portions of IDC's *Cyber Resilience Survey,* May 2026.

Cyber incidents are common
84.5% of organizations have suffered a cyber attack within the past 12 months. The plurality (33.8%) have suffered between one and five attacks, while the mean number of attacks over the past 12 months across all organizations is 11.3.

Data discovery and classification approach
34.5% classify consistently across most data types; 28.8% automatically across all data; 19.3% automatically across all data with regular auditing. Only 5.2% apply classification inconsistently.

Data access controls
45.8% automatically applied and aligned to data classification; 34.7% are automated in real time with auditing. Only 5.6% use manual controls with no classification link.

CRQ P&L approach
61.4% use a standardized taxonomy (e.g., FAIR model); 38.6% use proprietary internal benchmarks.

Threat modeling level
58.6% use standard threats plus organization-maintained ecosystem threats; 23.7% additionally incorporate industry-specific vertical intel; 17.4% rely solely on MITRE standards.

IRT (incident response team) documents
53.6% have living documents continuously updated and tested for critical internal functions;
26.9% continuously update but test quarterly; 17.4% test across all internal and external functions.
Only 2.0% have static documents.

Backup approach
53.1% have one backup solution covering most workloads; 26.9% have a fully integrated platform with unified policy management; 17.1% use multiple solutions per reference architecture; 2.8% have no reference architecture.

Role-based access control (RBAC)
46.9% have RBAC integrated with IAM/PAM with periodic review; 26.7% have dynamic RBAC supporting AI/analytics; 25.4% have standardized RBAC and review it occasionally; 0.9% have basic RBAC only.

Cryptographic key management
50.3% use the strongest encryption with regular key evaluation; 32.3% use the strongest encryption with frequent evaluation and a maintained framework; 17.1% use the minimum standards with regular evaluation.

Appendix (continued)

Clean point of recovery
52.7% use synthetic recovery or cleanrooms then manually align; 28.6% are fully integrated with recovery orchestration; 16.1% use synthetic tools for high-value workloads only; 2.6% rely entirely on manual processes.

Active directory/Entra ID protection capability
43.8% have advanced and integrated capability with well-defined recovery; 29.1% have automated capability with continuous improvement; 24.7% have documented and tested their capability; 1.5% have basic controls; 0.4% have informal/inconsistent capability.

Backup anomaly scanning
54.7% scan backups at ingest, upon restore, and periodically; 40.1% scan at ingest and restore only; 5.2% use signature-based scanning on ingest only. No backups go unscanned.

Tabletop testing exercises
34.9% conduct separate business/ops and technical tabletops 2+ times/year; 30.4% run 2+ cross-functional tabletops annually; 28.9% conduct multiple tabletop/cyber-range exercises with outside facilitators; 5.2% conduct one annual tabletop; 0.2% do not conduct any tabletop testing..

Penetration testing
51.6% conduct comprehensive pen testing but at a limited frequency; 43.8% conduct comprehensive and regularly scheduled pen testing; 4.5% conduct pen testing but with limited scope and frequency. No respondents reported no pen testing.

Overall incident response approach
50.6% have policies regularly updated and tested quarterly with leadership; 49.2% documented and tested annually. Virtually no one lacks formal plans (0.2% predefined but undocumented).

eDiscovery forensics capability
64.2% have eDiscovery applications automating business process and data management; 34.0% have full workflow automation, including project and document management; 1.7% have limited forensics; 0.2% have no capabilities.

Alternative communications during a crisis
55.1% have secure alternate communications contracted and regularly tested organization-wide; 36.5% are limited to cell networks; 7.4% have considered it but taken no action; 0.9% have not considered it.

Appendix (continued)

Data cleanrooms
44.5% have cleanrooms defined and provisioned but with sporadic testing; 40.1% have cleanrooms defined for critical data sets with documented runbooks; 13.4% have plans defined but not yet provisioned; 2.0% have not considered them.

Recovery point determination
54.5% automatically identify recovery points but apply them manually; 35.4% use granular, automatically determined recovery points feeding into a recovery orchestrator; 7.4% have manually determined recovery points with some granularity; 2.6% have manually determined recovery points and are limited to full backups.

Recovery automation level
42.5% have predominantly automated recovery with orchestrators for most recovery tasks; 39.9% make limited use of recovery orchestration; 9.6% have a mostly manual recovery process; 8.0% have a fully manual recovery process.

Runbooks for recovery
49.9% maintain runbooks updated annually or more; 26.5% have entirely manual runbooks updated irregularly; 19.7% use AI to dynamically generate and update runbooks; 3.5% have outdated runbooks; 0.4% have none.

Minimally viable organization (MVO) planning
56.2% have begun building an MVO plan; 42.1% have completed one; 1.5% are still considering; 0.2% have not considered it. Notably, 57.7% have not yet fully completed their MVO definition.

MVO recovery plans
54.0% drive recovery order jointly by IT and business needs; 37.5% are business-driven by criticality and risk tolerance; 7.6% are IT-driven only; 0.9% are entirely ad hoc.

IT security teams established
Network teams most prevalent (51.9%), followed by SecOps (48.8%), DevOps (45.5%), CloudOps (39.9%), ITOps (38.4%), and DevSecOps (36.7%). SOC (5.8%) and MDR teams (3.0%) are less common.

IT security team coordination
63.5% have governing groups for specific IT security functions; 22.1% coordinate informally on an as-needed basis; only 14.5% have an overall governing group for IT security.

Lead teams for IT security
SecOps most often leads coordination (32.1%), followed by DevOps (29.1%), network teams (27.8%), ITOps (27.6%), and CloudOps (22.6%).

Appendix (continued)

Governing group participants
Where an overall governing group exists: Network teams participate most (34.6%), DevOps (33.3%), SecOps (32.1%), ITOps (30.8%), CloudOps (29.5%), and DevSecOps (21.8%), with line-of-business reps included by 10.3%.

IT security collaboration improvement needed
49.7% say major improvements are needed; 29.5% say minor improvements are needed; 19.3% say a whole rethink is needed; only 1.5% say no improvement is needed, meaning 98.5% see room for improvement.

Executive leadership involvement in IT security
45.8% are actively involved; 27.3% are very actively involved; 26.2% are involved to an acceptable level. Less than 1% report limited or no involvement.

IT security policy development
56.6% have enterprise policies adopted but implemented manually; 31.4% use automated policy engines; 9.5% have formalized but siloed policies; 2.6% develop policies ad hoc.

IT security audits
59.7% conduct audits at least annually, mainly within the IT organization; 22.3% audit to C-level reporting requirements; 14.7% conduct limited-scope audits; 3.3% conduct audits only on an ad hoc basis.

About the IDC analysts

Phil Goodwin

Research Vice President, Infrastructure Software Platforms, Worldwide Infrastructure Research, IDC

Phil Goodwin is a research vice president within IDC's Worldwide Infrastructure Research organization and global research lead for the Infrastructure Software Platforms practice. He leads a team of analysts that provide detailed insights and analyses on evolving infrastructure software trends, vendor performance, and the impact of new technology adoption. Goodwin's own research focuses on multi-cloud data management, data logistics, on-premises and cloud-based data protection as a service, cyberprotection and recovery, and recovery orchestration. He takes a holistic view of these markets and covers risk analysis, service-level requirements, and cost/benefit calculations in his research. Goodwin also contributes regularly to IDC's CIO Advisory practice.

More about Phil Goodwin →

Craig Robinson

Research Vice President, Security Services, IDC

Craig Robinson is a research vice president within IDC's Security Services research practice, focusing on managed services, consulting, and integration. Coverage areas include managed detection and response services, cyber-resilience, and incident readiness and response services. Robinson delivers unparalleled insight and analysis, leveraging his unique practitioner experience leading diverse IT teams across several industries. This expertise positions him to provide valuable thought leadership, research, and guidance to vendors, service providers, and clients worldwide.

More about Craig Robinson →

About the IDC analysts (continued)

Frank Dickson

Group Vice President, Security and Trust, IDC

Frank Dickson is the group vice president for IDC's Security and Trust research practice. In this role, he leads the team that delivers compelling research in the areas of AI security; cybersecurity services; information and data security; endpoint security; trust; governance, risk, and compliance; identity and digital trust; network security; privacy and legal tech; and application security and fraud. Topically, he provides thought leadership and guidance for clients on a wide range of security topics, including ransomware and emerging products designed to protect transforming architectures and business models.

More about Frank Dickson →

Message from the sponsor

This research is offered by Commvault to advance how business, IT, and security leaders prepare for, withstand, and recover from disruption.

Commvault is a leader in unified resilience at enterprise scale. Customers trust Commvault to conduct the fastest, most complete recoveries, not just of their data, but their entire business. Purpose-built for the agentic enterprise, Commvault unifies data security, identity resilience, and cyber recovery on one cloud-native, AI-enabled platform.

Through Commvault® Cloud, business, IT, and security teams gain a shared way to protect critical data, defend against attacks, and recover clean across cloud, on-premises, and hybrid environments.

Learn how Commvault helps organizations stay resilient and moving forward.

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

IDC.com | IDC on LinkedIn | IDC Blog

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.