Deloitte.

In association with **Rubrik**

RANSOMWARE AS A BUSINESS-CRITICAL THREAT: ***WHY IDENTITY RESILIENCE DETERMINES RECOVERY OUTCOMES***

EXECUTIVE SUMMARY

Ransomware is an evolving attack vector that continuously forces the cybersecurity landscape to shift with it, driving costly operational outages and prolonged recoveries that cascade across an organization. In a recent survey, 78% of organizations reported they were very or extremely prepared to mitigate an attack, yet 50% still fell victim to ransomware in the last year[1]. This pivots the conversation away from attack prevention toward organizational resilience to withstand the impact of an attack. Downtime can cost up to $6,000 per minute, and the financial impact is often driven more by disruption and recovery than by the ransom itself, with lost productivity, extended outages, and system rebuilds accounting for much of the total cost[2].

To maximize the disruption and extend recovery timelines, attackers increasingly target the very systems organizations rely on to bounce back – backups and identity. In 2025, identity-based attacks made up 80% of total intrusions, highlighting how often attackers focus on access and authentication as a pathway to disrupt recovery[3]. Attackers try to undermine victims' ability to recover by disrupting access to data and authentication. Compromising identity systems also helps them move faster inside the organization, accelerating privilege escalation and disabling security. Increasingly, attackers are taking advantage of this tactic. In an external survey, 78% of human-operated attacks breached a domain controller, which compromised identity and privileged access[4].

A common misconception is that "identity will be fine" because it's delivered as software as a service (SaaS). In practice, SaaS availability is not the same as enterprise recoverability; and even with a provider, the organization remains accountable for the recoverability of its identity forest, configurations, and dependencies. Ultimately, identity resilience should be treated as a core cyber recovery capability, with clear ownership to ensure authentication can be restored quickly under attack.

THE TRUE COST OF RANSOMWARE:
DISRUPTION, NOT DEMANDS

Ransomware response has become a leadership stress test for Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs). Beyond extortion pressure, teams must restore operations quickly, re-establish trust in systems and users, and meet legal and regulatory expectations, often while forensic uncertainty remains.

Critically, identity is now a "stop-the-business" dependency that can materially extend outages and inflate recovery costs. Even when infrastructure and applications can be technically restored, recovery can stall if administrators, responders, and employees cannot authenticate or re-enable essential controls. When identity is degraded, response teams can lose administrative access, security tooling may be disabled or untrusted, and recovery can become slower, riskier, and more expensive, even if backups exist.

This risk is often underestimated in cloud-first environments. Many organizations assume that because identity is delivered as SaaS, recovery will be automatic and end-to-end. However, in reality, the provider may restore platform availability while the organization still has to restore configurations, integrations, and operational workflows. Mitesh Shetty, a managing director in Deloitte & Touche LLP's Cyber Resilience practice, shared "there is an explicit expectation that because it is a SaaS solution, it will always be available which is a wrong assumption that clients need to think about." To that point, Vivek Lodhi, a managing director in Deloitte & Touche LLP's Identity practice emphasized, "A lot of these SaaS solutions offer their own disaster recovery (DR) support as part of an advanced solution that clients can buy, but their solutions focus primarily on the availability of services and infrastructure recovery. It does not fully address the resilience and data recovery aspects."

THE IDENTITY-RANSOMWARE LINK:
HOW ATTACKERS STOP RECOVERY

Ransomware operators increasingly target identity infrastructures (e.g., network database management and cloud authentication platforms) because it is the fastest path to scale impact. Compromising identity enables them to:

- ***Escalate privileges and move laterally at speed***
- ***Disable or evade security tooling and logging***
- ***Lock out administrators and responders, delaying containment and recovery***
- ***Sabotage restoration workflows, including backup recovery and service reactivation***

At an enterprise-level, keeping recovery points trustworthy starts with assessing gaps that could undermine recovery, then designing and implementing a pragmatic recovery plan to address them. This is no longer a passive "encrypt and wait" model; attackers increasingly target recovery dependencies – especially identity and backups.

Rubrik, a leading cybersecurity company, helps clients fortify their systems against identity and data attacks with their unified platform for data protection and ransomware recovery. Rubrik Identity Solutions Engineer David Smith has seen attackers directly dismantle recovery paths by "gaining access to password vaults, deleting backups, and deploying ransomware to virtual machines, which shut it all down." He stressed how "critical it is for organizations to understand what their posture is, and understand how they can be resilient before an attack." Shetty agreed, emphasizing that attackers' primary focus is "to get access to the domain controller or identity solution since when they have that they have the keys to the kingdom."

WHAT MATTERS MOST:
PRIORITIES FOR RANSOMWARE RECOVERY RESILIENCE

Resilient organizations move beyond generic leading practices and focus on recovery outcomes that are measurable, testable, and executable under pressure.

PRIORITIZE MISSION-CRITICAL SERVICES WITH MINIMAL VIABLE COMPANY (MVC) PLANNING

Organizations that identify and rank services and datasets required to operate as a minimum acceptable level are better able to prevent over-engineering, clarify recovery sequencing, and align resilience investment to business impact. Recovery is rarely a clean, all-at-once restoration, as there are typically constraints on what can be safely brought back online first. To that end, Shetty emphasized the need to pre-align on what matters most. He expanded on this concept by stating "Understanding what is really important to run the business and focusing on that as your starting point can help you achieve the right amount of coverage."

Put simply, if you haven't decided what comes back first, ransomware will decide for you.

CONTINUOUSLY TEST AND HARDEN RECOVERY PROCESSES (NOT JUST BACKUPS)

Ransomware frequently impacts production systems and the dependencies required to restore them. Recovery plans should be validated through scenario-driven testing that proves teams can authenticate, coordinate, and execute quickly – even when identity is partially degraded. As Smith put it, "A lot of organizations need to do a simulated recovery, a lot might do it as a tabletop exercise and think they can do certain things, but then they don't realize the dependencies on something like identity or other applications they are not thinking about." Tabletops help alignment, but recovery readiness requires hands-on validation, access paths, runbooks, escalation routes, and decision rights must work as designed.

BUILD RESILIENT IDENTITY AND ACCESS STRATEGIES

Because identity compromise can halt recovery, resilience requires both strong preventive controls and explicit lockout readiness. Lodhi stated, “The attacks that we see [most] are compromised admin credentials…once an attacker gains privileged access, it’s easy for them to engineer their way through and access private details.” That reality makes it essential to design identity and access so failures are contained, and recovery can proceed.

Core elements of a resilient identity system include:

Layered access controls:
least privilege, role-based access, frequent permission reviews

Lockout playbooks:
escalation routes, re-verification workflows, documented emergency procedures

Removal of single points of failure:
multiple multi-factor authentication options, alternate recovery paths

Break-glass access:
offline-secured privileged accounts, limited custodians, auditable use, periodic testing

SAFEGUARDING IDENTITY AND DATA:
CAPABILITIES THAT ENABLE RECOVERY UNDER ATTACK

Identity resilience depends on the ability to restore a trusted "last-known-good" state without reintroducing attacker changes – and to do so quickly in order to restore business operations as soon as possible. Organizations build recovery confidence over time by continuously monitoring and controlling readiness (including identity-change activity) and by testing their plans in realistic scenarios.

Key enabling capabilities to restore quickly include:

- ***Isolated and immutable backups to protect recovery points from tampering***
- ***Identity change visibility (time-stamped tracking) to support faster triage and cleaner restoration decisions***
- ***Granular rollback to remove malicious changes without reverting the entire environment unnecessarily***
- ***Recovery orchestration to reduce manual error and compress timelines across data, systems, and identity dependencies***

Organizations with intentionally designed and implemented identity resilience across their IT security workflows are typically able to restore authentication and privileged access more quickly and safely following an attack. Smith highlighted how a cohesive identity recovery solution can support these capabilities. "Having the ability with an activity log to see all the changes in a backup is a huge advantage. It's really rolling back and granularly removing those changes that's critical to quick recovery, so you don't have to restore back [multiple] days." This kind of control over backups and changes is a game-changer when it comes to confidence in an organization's recoverability. But, that is only one piece of the puzzle.

Siloed or multi-point solutioning—which require specific, niche solutions for every system—are costly and can result in longer recovery times. Shetty stressed how recovery orchestration is most effective when there is a cohesive recovery strategy across critical systems. He shared, "when you are in recovery, multiple point solutions are going to make your recovery longer, so you need to look at an enterprise view to simplify recovery…using a unified solution is going to be a key aspect." Andreas Laxgang, an Identity and Cloud Security specialist at Rubrik, noted that the market has been swinging between extremes: multi-point "best-in-class" solutions were popular for years, but consolidation has accelerated as organizations try to reduce complexity. Yet, the likely end state isn't purely one or the other. As he put it, "there was a big push for consolidation, and now it's going to be a hybrid model… you want best of breed solutions that speak to one another." In practice, it's not about one platform vs. many tools, it's about an integrated recovery approach teams can effectively execute.

CONCLUSION

Many organizations assume their identity provider will “handle resiliency” during an incident. In reality, providers typically restore platform availability, not the organization’s end-to-end recoverability across configurations, integrations, privileged access pathways, and business workflows.

Organizations remain accountable for:

- *Defining MVC outcomes and recovery sequencing*
- *Testing lockout scenarios and privileged access restoration*
- *Establishing identity recovery ownership and decision rights*
- *Ensuring identity recovery is integrated with cyber recovery operations*

For many organizations, the practical goal is not a “perfect” restore, it is a trusted, last known-good identity state that can be re-established quickly and safely without reintroducing attacker changes. That requires visibility into identity changes and recovery orchestration that reduces manual effort when teams are operating under pressure. In Deloitte’s recovery work, this “trusted state” is typically made concrete through clear recovery decision points and rehearsed steps for re-enabling privileged access.

Deloitte helps organizations treat identity resilience as a core cyber recovery discipline. Much like Shetty and Laxgang, Lodhi is also “seeing a preference in centralized solutions.” As he put it, “clients want to build resiliency as part of their enterprise, not just purely identity solutions… and that’s where I can see Rubrik coming in.” By pairing identity and cyber resilience planning with recovery capabilities that support restoring trusted identity states and re-enabling access, organizations can execute a tested, business-aligned recovery strategy when it matters most.

WHAT NEXT?

Facing emerging operational challenges and evolving cyber threats?

Implement resilient recovery solutions with a unified, scalable, and secure data management approach that simplifies operations, improves recovery times, and integrates with cloud environments.

Together, Deloitte and Rubrik can support your journey, working side by side from data strategy and resilience architecture to orchestrated recovery and integration with enterprise risk management tools—tailored to your business needs. Let's get started.

LEARN MORE

GET IN TOUCH

MIKE KOSONOG
Rubrik Alliance Relationship Lead, Cyber Resilience Market Offering
Deloitte & Touche LLP
mkosonog@deloitte.com

MITESH SHETTY
Managing Director, Cyber Resilience Practice
Deloitte & Touche LLP
mishetty@deloitte.com

SHARON CHAND
US Defense and Resilience Leader
Deloitte & Touche LLP
shchand@deloitte.com

VIVEK LODHI
Managing Director, Identity Practice
Deloitte & Touche LLP
vilodhi@deloitte.com

ROB JOSEPH
Global Alliance Manager
Rubrik
rob.joseph@rubrik.com

LAUREN BROOKS
Senior GSI Account Executive
Rubrik
lauren.brooks@rubrik.com

ANDREAS LAXGANG
Identity and Cloud Security Specialist
Rubrik
andreas.laxgang@rubrik.com

DAVID SMITH
Solutions Engineer
Rubrik
david.smith@rubrik.com

REFERENCES

i. Fortinet. "Fortinet Survey Finds 78 Percent of Organizations Felt Prepared for Ransomware, Half Still Fell Victim." Fortinet Newsroom (press release). Accessed January 30, 2026.

ii. Rubrik Zero Labs. "The State of Data Security: A Distributed Crisis." Accessed January 30, 2026.

iii. IBM X-Force. X-Force 2025 Threat Intelligence Index. IBM, 2025. Accessed January 30, 2026.

iv. Microsoft. "How Cyberattackers Exploit Domain Controllers Using Ransomware." *Microsoft Security Blog*, April 9, 2025. Accessed January 30, 2026.