Five reasons why identity resilience is the new executive imperative

In a world of inevitable breaches and expanding identities, resilience depends on how well leaders govern, secure and recover access

Cyber risk has evolved beyond a technical concern. Identity now underpins operational continuity, regulatory compliance and organisational readiness for AI. As human, machine and automated identities multiply, the ability to govern and secure them has become a board-level responsibility.

In today's high-risk environment, breaches are on the rise and no organisation is immune. Resilience is no longer defined by prevention alone, but by how quickly and confidently organisations can recover when it happens. Yet recognising this reality is the first step towards meaningful action. This shift in mindset defines modern leadership — and explains why identity has become an executive imperative.

Here are five reasons identity resilience urgently demands board-level attention.

32%

The rise in identity-based attacks in the first half of 2025

50%

of cyberattacks with known motives had financial objectives such as ransom or extortion

Microsoft, 2025

1 Identity failures are business failures

A single compromised identity can cascade from an internal disruption into widespread operational and financial damage. Identity attacks increasingly target access pathways rather than infrastructure, making them harder to detect and faster to escalate.

40%

of ransomware attacks now target both on-premises and cloud systems, increasing the potential impact

17%

of cyberattacks involve attackers using legitimate accounts to access systems, making breaches harder to detect

Microsoft, 2025

2 Regulation leaves no room for oversight

Cyber resilience regulation is tightening worldwide, with senior leaders increasingly accountable and organisational preparedness under scrutiny. Identity governance, access control and recoverability are now critical under the UK's Cyber Security and Resilience Bill, which now enables fines of up to £17 million or 4% of annual global turnover, EU frameworks like NIS2 and DORA, the US Cyber Incident Reporting for Critical Infrastructure Act and expanding Asia-Pacific requirements.

3 AI is multiplying identities faster than governance can keep up

AI is being adopted faster than ever, and with it, new types of identities are multiplying — specifically non-human identities such as service accounts, bots and automated agents. These identities often have high-level access but little oversight, which makes them a major security risk if not properly managed. With over half of organisations saying non-human identities are the hardest to secure, AI-driven scale is outpacing governance at an alarming rate — turning identity into one of the fastest-growing security blind spots.

50%

of organisations report that non-human identities are the hardest to secure

Quest, 2026

4 AI scales risk as fast as it scales efficiency

Over 80% of organisations believe AI can strengthen security operations, from faster threat detection to improved response times. But AI does not fix weak foundations — it amplifies what already exists. In identity governance, that means AI can rapidly scale access and decisions beyond human oversight if controls over service accounts, bots and automated agents are not in place. Strong identity controls are essential to ensure AI scales safely, not dangerously.

80%

of organisations believe AI can enhance identity threat detection and response

Quest, 2026

5 Recovery, not prevention alone, defines true resilience

Identity now connects every dimension of modern resilience: security, compliance, recovery and AI readiness. Positioning it solely within IT as a technical issue leaves organisations exposed. By elevating identity resilience to the boardroom and embedding a robust recovery strategy, firms can unlock organisational agility, strengthen trust and make identity a strategic safeguard for the business in an AI-driven world.

Only **24%**

of organisations test disaster recovery plans every six months

Quest, 2026

Given the success of cyberattacks, a breach is a question of when, not if. Yet only one quarter of organisations test their disaster recovery plans every six months, leaving most unprepared to rapidly and safely restore identities, access and trust. Restoring identity and access controls are essential to assure business continuity, safeguard customers and stay compliant.

To learn how to protect the full identity lifecycle, from rapid detection and response to recovery up to 90% faster, saving organisations millions in downtime costs, visit Quest Software.