HUMAN ERROR

David Baggett *explores cyber security's biggest unsolved problems, courtesy of Kaseya's 2026 Cybersecurity Report*

Kaseya has released its Cybersecurity Report: Building Security That Survives Human Error, the most comprehensive look yet at how cybersecurity is really being practiced on the ground. Based on responses from 1,132 MSPs and IT professionals across more than 60 countries, the research cuts through the theory to examine what is getting in the way of good security.



Human error, including social engineering and distraction, ranks as the top threat vector 68 percent of respondents are most concerned about in the next 12 months, followed by email at 55 percent. Among organisations that experienced an incident in the past three years, four of the top five contributing factors were people related, led by poor user practices or gullibility (41 percent) and a lack of end-user cybersecurity training (40 percent). The findings suggest that despite advances in security technology, people remain one of the most difficult vulnerabilities for organisations to address.

People aren't perfect, and everyone knows it. Yet much of cybersecurity still depends on people making the right decision every time. The path to true cyber resilience isn't about eliminating mistakes. It's about building an organisation that can withstand them. Expect mistakes, account for constraints and engineer around them.

Nearly 65 percent of respondents say they could pass a compliance audit today without preparation; but that confidence may be optimistic. When asked what could create problems during an audit, 49 percent pointed to incomplete documentation or policies, followed by security controls that are not fully implemented (34 percent) and a lack of employee security awareness or training (33 percent).

Only 20 percent of IT departments say their cybersecurity budget is growing in line with real risk. At the same time 77 percent of those surveyed describe themselves as under-resourced in some way: budgets held flat while threats grow (23 percent), growing but too slowly to keep pace (30 percent), or under-resourced and aware of it (24 percent). MSPs report a similar pattern among their client base, with 65 percent saying clients are underinvested in cybersecurity relative to their risk.

Alongside these findings, Kaseya is introducing an MSP resilience assessment, giving MSPs visibility into what high-performing companies do differently. High and low performers were defined by whether they met both revenue and growth goals over the last two quarters.

The assessment shows that high performing MSPs have turned compliance, cyber insurance and AI adoption into competitive advantages, while low-performing MSPs – often constrained by budget or size – deprioritise those same areas.

Incident response and backup testing: Almost 30 percent of high-performing MSPs test their clients' incident response plans quarterly, compared with 18 percent of low-performing MSPs. Only 11 percent of high-performing MSPs report not having an incident response plan, compared with 25 percent of low-performing MSPs. Across all MSPs, 15 percent do not have an incident response plan.

Compliance as a differentiator: High-performing MSPs are making compliance a more meaningful part of their business. A quarter generate 11–25 percent of their revenue from compliance services, compared with 15 percent of low-performing MSPs, suggesting that compliance can be a strong differentiator and revenue opportunity.

Tech stack depth: While foundational tools like EDR, MFA, BCDR and email security are near-universal across all MSPs, high performers pull ahead on advanced, proactive layers, including SIEM adoption (48 percent high vs. 42 percent all vs. 31 percent low), NDR (52 percent top vs. 44 percent all vs. 27 percent low) and cloud security/CNAPP (32 percent high vs. 22 percent all vs. 13 percent low).

The report closes with a five-part playbook for building resilience into daily operations: designed for the mistakes teams already expect, making the case for investment before an incident forces the issue, removing friction so secure behavior is the easy choice, using AI to extend stretched teams, and treating compliance as continuous work rather than a once-a-year scramble ●

77 percent of IT departments surveyed say that they are under-resourced

David Baggett is SVP and GM, Security Suite, Kaseya